Пензенский государственный университет
ФГУП Пензенский научно-исследовательский электротехнический институт
Пензенский филиал ФГУП НТЦ «Атлас»
Филиал ФГУП ПНИЭИ научно-исследовательское предприятие «Аргус»
Пензенское научно-исследовательское предприятие «Сталл»
Научно-производственная фирма «Кристалл»

Труды научно-технической конференции
Вебсайт http://beda.stup.ac.ru/RV-conf/

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ТОМ 4.

Пенза-2003 г.

УДК: 681.322

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Труды научно-технической конференции под редакцией Волчихина В.И., Зефирова С.Л. - Пенза - 2003. Издательство Пензенского научно-исследовательского электротехнического института. Том 4. 95 С.

Рассматриваются проблемы безопасности информационных технологий. Приведенные материалы отражают дискуссию по затронутой тематике, возникшую на научно-технической Internet конференции, непрерывно проводимой на сервере Пензенского государственного университета http://beda.stup.ac.ru/RV-conf. Представлены материалы, поступившие в оргкомитет в период с января по декабрь 2004 года. Том 4 содержит 22 статей, отражающих точку зрения 21 специалистов по различным аспектам информационной безопасности.

ПОЧТОВЫЙ АДРЕС ОРГКОМИТЕТА: Россия 440024, г. Пенза, ул. Красная, 40. ПензГУ. Кафедра ИБСТ, RV-конференция. **E-mail** оргкомитета: rv-conf@beda.stup.ac.ru, сервер конференции http://beda.stup.ac.ru/RV-conf/

Состав оргкомитета научно-технической конференции

Председатель – Волчихин Владимир Иванович, докт. техн. наук, проф., ректор Пензенского государственного университета

Сопредседатель - Зефиров Сергей Львович, доцент, канд. техн. наук, зав. каф. «Информационная безопасность систем и технологий» Пензенского государственного университета.

ЧЛЕНЫ ОРГКОМИТЕТА:

Овчинкин Г.М., канд. техн. наук., научный директор Пензенского научно-исследовательского электротехнического института (ПНИЭИ).

Чижухин Г.Н., докт. техн. наук, зам. директора по науке Пензенского филиала ФГУП НТЦ «Атлас».

Андрианов В.В., член-корр. Академии Криптографии РФ, канд. техн. наук., научный руководитель Научно-производственной фирмы «Кристалл».

Селезнев Г.Б., канд. техн. наук., зам директора по науке Филиала ФГУП ПНИЭИ научно-исследовательского предприятия «Аргус»

Николаев В.Ю., директор ПНИП «Сталл»

СЕКЦИИ

1. Концептуальные основы информационной безопасности и проблемы информационного противоборства
2. Информационная безопасность сложных систем
3. Нормативное, методологическое и методическое обеспечение информационной безопасности
4. Анализ вычислительной среды, верификация, сертификация программ
5. Управление информационной безопасностью
6. Системы обнаружение вторжений
7. Аудит информационной безопасности
8. Конфиденциальность, целостность, доступность
9. Аутентификация: парольная, биометрическая, криптографическая

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.3-6. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/001)

БИОМЕТРИЧЕСКИЕ И НЕЙРОСЕТЕВЫЕ МЕХАНИЗМЫ СВЯЗИ С КРИПТОГРАФИЧЕСКИМИ МЕХАНИЗМАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Иванов А.И. Лаборатория биометрических и нейросетевых технологий Пензенского научно-исследовательского электротехнического института

Криптография является единственной технологией, позволяющей надежно защитить человека (его права, его имя, его информацию, его электронные деньги,…) в открытом информационном пространстве (например, в ИНТЕРНЕТ). Однако пользоваться криптографией неудобно. Пользователь лишен мобильности, ему приходится хранить криптографические ключи в сейфе (спецотделе), банке. Эта ситуация отображена на рисунке 1. Из-за этого пользователи стараются избегать применения криптографической защиты. Снижается общий уровень защищенности информационного общества.

Обычная технология криптографической аутентификации человека в открытом информационном пространстве

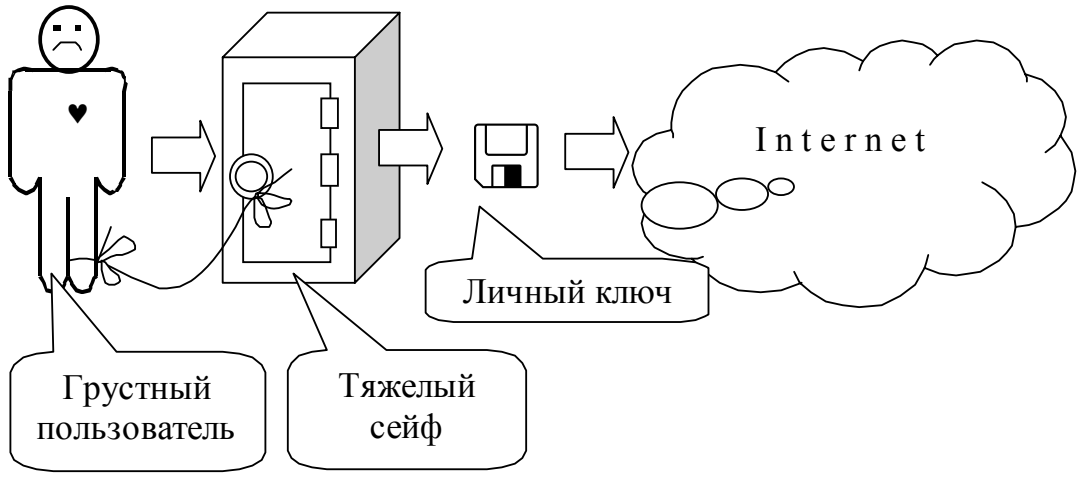


Рисунок 1.

Трудно себе представить, что каждый человек для осуществления значимой операции будет идти к сейфу в банке или спецотделе, извлекать ключевую дискету, осуществлять криптографическую операцию и возвращать дискету в сейф. Это ситуация скорее теоретическая нежели практическая. Сейф – это крайне неудобная и тяжеловесная форма хранения криптографических секретов.

Пензенский электротехнический в инициативном порядке разрабатывает новую гораздо более удобную для пользователей технологию хранения криптографического ключа. Эта технология отображена на рисунке 2 и сводится к использованию программных эмуляторов искусственных нейронных сетей.

Новая технология криптографической аутентификации в открытой системе

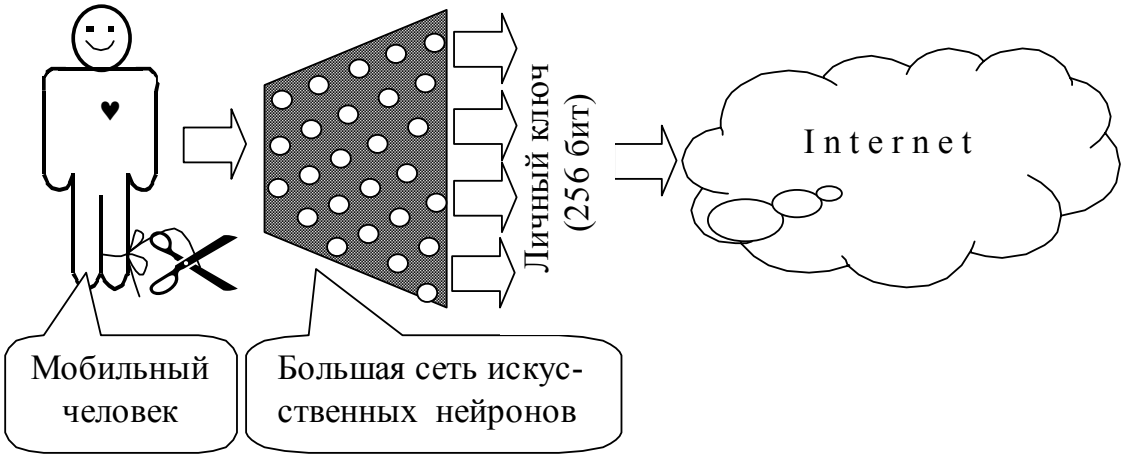


Рисунок 2.

Как видно из рисунка пользователь уже не привязан к сейфу. Его ключ храниться в структуре и связях большой нейронной сети, программный эмулятор которой может храниться открыто (на дискете или в компьютере). Пользовать может в любой момент предъявить свой биометрический образ (например, автограф), параметры которого нейронной сетью превращаются в ключ. Ключ как токовой не хранится в компьютере, храниться только нейросеть воспользоваться которой может только тот, кто обладает нужной биометрией.

В качестве индивидуальных биологических параметров могут использоваться различные измеримые признаки. Присутствующие на рынке биометрические методы распознавания человека имеют разную стоимость и разные технические характеристики (разные вероятности ошибок первого и второго рода). Взаимное сравнение биометрических технологий может быть достаточно просто осуществлено по их эффективности. При оценке эффективности возникают определенные трудности связанные с тем, что ошибки первого и второго рода для разных технологий существенно разнятся. Однако эту проблему можно решить если считать, что вероятности ошибки биометрических технологий первого рода (ошибочного отказ «Своему») примерно одинаковы и находятся на уровне 0,01. При этом предположении биометрические системы можно сравнивать по вероятностям ошибок второго рода (вероятностям пропуска «Чужого»). Тогда эффективность биометрических систем будет тем выше, чем меньше их стоимость и тем выше, чем меньше вероятность ошибок второго рода.

Сравнение всех известных технологий [1] по их эффективности показывает, что присутсвующие сегодня на биометрическом рынке технологии неэффективны. Они дороги и имеют вероятность ошибки второго рода на уровне $10^{-7}…10^{-12}$. Дальнейшее снижение вероятности ошибки второго рода проблематично, так как наталкивается на физические ограничения, присущие уникальности открытых и неизменных образов человека (отпечаткам пальцев, рисунку глазного дна,…)

Более эффективными являются технологии, построенные на использовании особенностей организации естественного интеллекта личности человека. Первая причина высокой эффективности этих технологий состоит в том, что они при их чисто программной реализации могут иметь очень низкую стоимость. При этом предполагается, что устройства ввода данных (рукописной графика и голоса) в защищаемых компьютерах уже имеются (широко

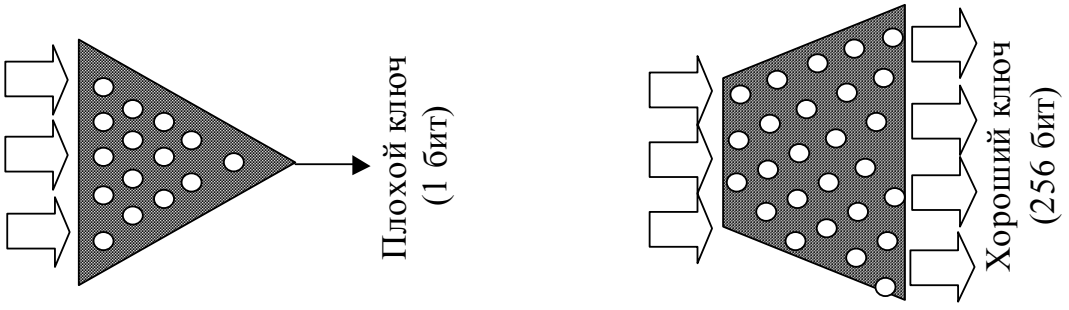
распространены звуковые карты, зачастую карманные компьютеры не имеют клавиатуры, но имеют перьевой ввод рукописной информации).

Вторая причина высокой эффективности состоит в том, что рукописные или голосовые биометрические образы могут быть сделаны тайными. В этом случае злоумышленник не может заранее изготовить муляж и вынужден заниматься подбором биометрических образов. Оценки стойкости тайных биометрических образов дают величины вероятности ошибок второго рода 10^{-33} на слове из 5 рукописных букв. Увеличение длинны тайного рукописного слова дает соответствующее снижение вероятности ошибки второго рода. Теоретически эта ошибка может быть сделана как угодно малой за счет увеличения длинны рукописной парольной фразы.

Когда биометрические образы известны всем их могут попытаться подделать, например, изготовить их муляж. Соответственно рядом с биометрической системой должна появиться охрана, контролирующая корректное использование биометрии пользователями. Необходима физическая защита статической биометрии с один раз заданными и никогда не изменяемыми биометрическими образами.

Иначе обстоит дело при использовании свободно изменяемых (динамических) биометрических образов. При вероятной компрометации тайны биометрического образа он может быть оперативно изменен на другой образ. Кроме того длина динамического биометрического образа может быть любой, что позволяет теоретически неограниченно увеличивать стойкость биометрической системы к взлому. Вместо одного рукописного (голосового) слова-пароля может быть использована несколько слов (парольная фраза). Длинна тайной парольной фразы, порядок написания знаков, уникальность почерков в конечном итоге и определяют стойкость системы к попыткам ее преодоления.

Реализация программной защиты высокой стойкости



Слабая программная защита

Сильная программная защита

Рисунок 3.

Еще раз подчеркнем, что высокая эффективность программной защиты обусловлена специальными мерами безопасности. Эта ситуация отображена на рисунке 3. Обычные программы защиты информации, имеющие последний решающий бит всегда имеют низкую стойкость. Хакер находит и искажает

последний бит, программа начинает выполнять обратную функцию. Для исключения этой ситуации необходимо использовать искусственную нейронную сеть с большим числим выходов.

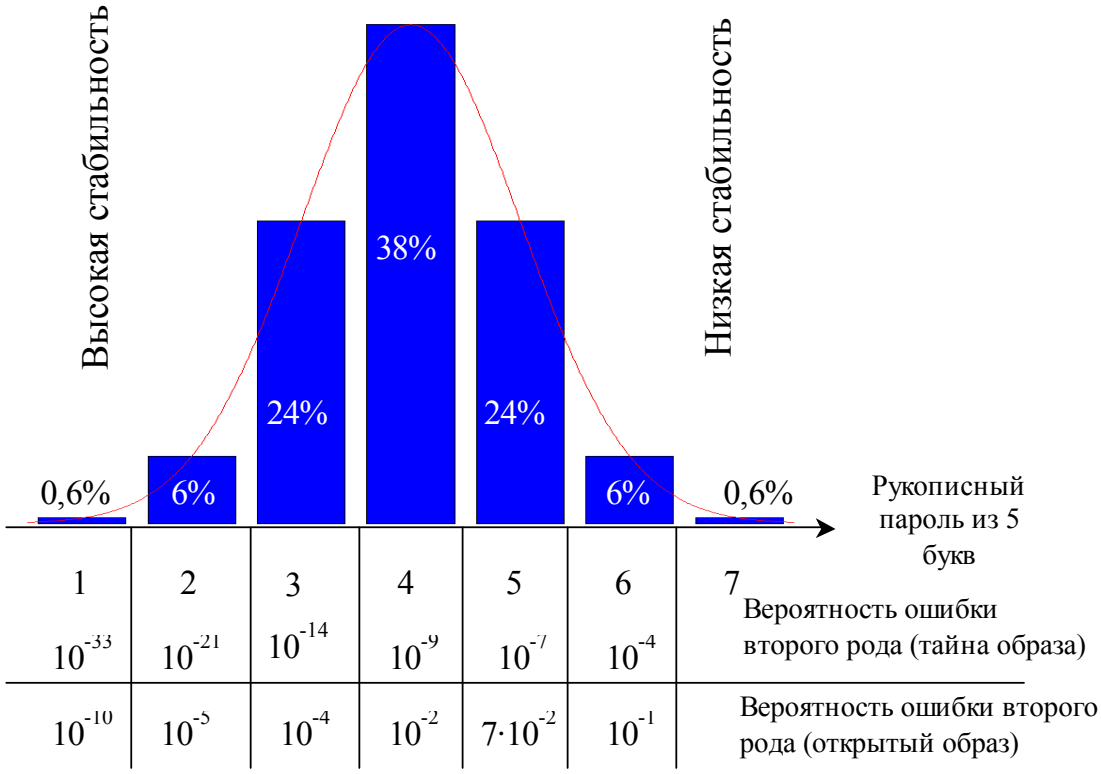


Рисунок 4.

Статистические характеристики коммерческой системы «Нейрокриптон» [2] отображены на рисунке 4. Все люди по стабильности рукописного почерка делятся на 7 групп. Система автоматически классифицирует пользователей. Наиболее стабильным почерком обладают люди относящиеся к первой группе. Для них вероятность ошибочного пропуска «Чужого» не знающего написания рукописного пароля оказывается на уровне 10^{-33}, что более чем достаточно для практического использования.

ЛИТЕРАТУРА

1. Иванов А.И. Оценка эффекта от использования тайных биометрических образов. //Защита информации. Конфидент. 2002. с.128-131.
2. Ефимов О.В., Иванов А.И. Программные хранители паролей с биометрическим доступом. //Современные технологии безопасности. 2002, № 2. с. 30-32.

Материалы поступили 12.04.2003. Опубликовано в Internet 30.06.2003

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.7-10. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/002)

ПРОТИВОДЕЙСТВИЕ ПОПЫТКАМ ПЕРЕХВАТА ПАРОЛЬНОЙ ФРАЗЫ ПРИ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО ГОЛОСУ

Болдырев С.Г.
ПНИЭИ. Лаборатория биометрических и нейросетевых технологий.

Идентификация личности по особенностям голоса имеет ряд привлекательных сторон. Во-первых, существует хорошо развитая телефонная сеть, во-вторых, звуковые карты фактически стали стандартным оборудованием современных персональных компьютеров. Кроме того, идентификация по голосу является традиционной для людей и не вызывает психологической неприязни. Однако биометрические системы идентификации человека по особенностям его голоса и индивидуальным параметрам его голосового тракта обладают большим недостатком, заключающимся, прежде всего в том, что парольную фразу трудно сохранить в тайне.

Современные средства акустического прослушивания ("радио-жучки" и другие прослушивающие устройства) позволяют достаточно успешно осуществлять несанкционированное копирование парольной фразы и последующей имитации голоса. В заявке на патент РФ [1] предложен способ потенциального противодействия "магнитофонам", основанный на использовании дополнительной речевой информации, вводимой с ларингофона, контактирующего с телом говорящего. Отсутствие сведений о зоне съема сигнала усложняет злоумышленнику преодоление систем биометрической идентификации человека, т.к. речевой сигнал, поступающий с ларингофона, и соответствующие ему параметры речевого сигнала зависят от местоположения ларингофона и не могут быть воспроизведены современными техническими средствами. Сигнал с ларингофона нельзя описать с достаточной степенью точности современным математическим аппаратом из-за сложности динамических модулей, учитывающих форму и структуру мышц, хрящей, костей и т.п. при их взаимодействии между собой.

Биометрическая идентификация личности по голосу, с использованием ларингофона заключается в следующем [2]. При произношении речевой сигнал в виде колебаний распространяется на мышцы человека, его ткани, сосуды, кожу и кости. Эти колебания представляют собой фонический сигнал тракта звукопередачи тела человека. При идентификации сигналы снимаются с выбранных зон съема сигнала. На рисунках 1,2 изображены фонические сигналы, снятые с разных зон при одной и той же функции возбуждения.

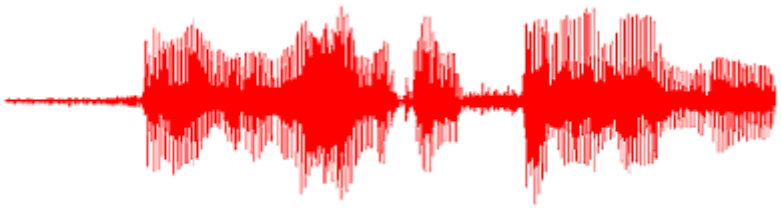


Рисунок 1.

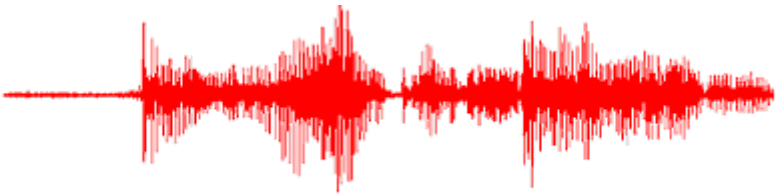


Рисунок 2.

Из рисунков видно, что сигналы отличаются друг от друга, так как у каждого из них свой тракт звукопередачи. Тракт звукопередачи отдельной зоны включает в себя различные кости, мышцы, сосуды человека, встречающиеся на пути распространения сигнала. Все зависит от выбранной зоны съема фонических сигналов. На рисунке 3 представлены используемые зоны съема фонических сигналов.

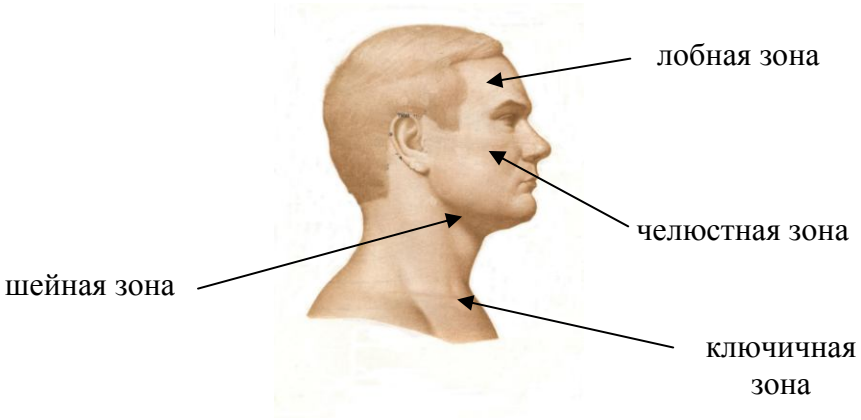


Рисунок 3.

В результате экспериментальных исследований, заключающихся в идентификации дикторов по разным зонам съема фонических сигналов относительно собственных и чужих эталонов, была получена статистическая оценка, на ограниченном наборе измерений. В исследованиях использовалось по 100 произношений для "Чужого" с каждой зоны съема сигналов и 70 произношений для одной зоны съема сигналов у "Своего". Результаты испытаний идентификации нашли отражение в графиках распределения значений меры Махалонобиса для "Своего" и "Чужого". Графики распределений значений меры для различных зон съема фонических сигналов приведены на рисунке 4,
где

– f_s1(x) – функция распределения значений квадратичной меры Махалонобиса для "Своего" при лобной зоне съема фонических сигналов;

– f_ch1(x) – функция распределения значений меры для "Чужого" при лобной зоне съема сигналов;

– f_ch2(x) – функция распределения значений меры для "Чужого" при челюстной зоне съема сигналов;

– fch3(x) – функция распределения значений меры для "Чужого" при шейной зоне съема сигналов;

– fch4(x) – функция распределения значений меры для "Чужого" при ключичной зоне съема.

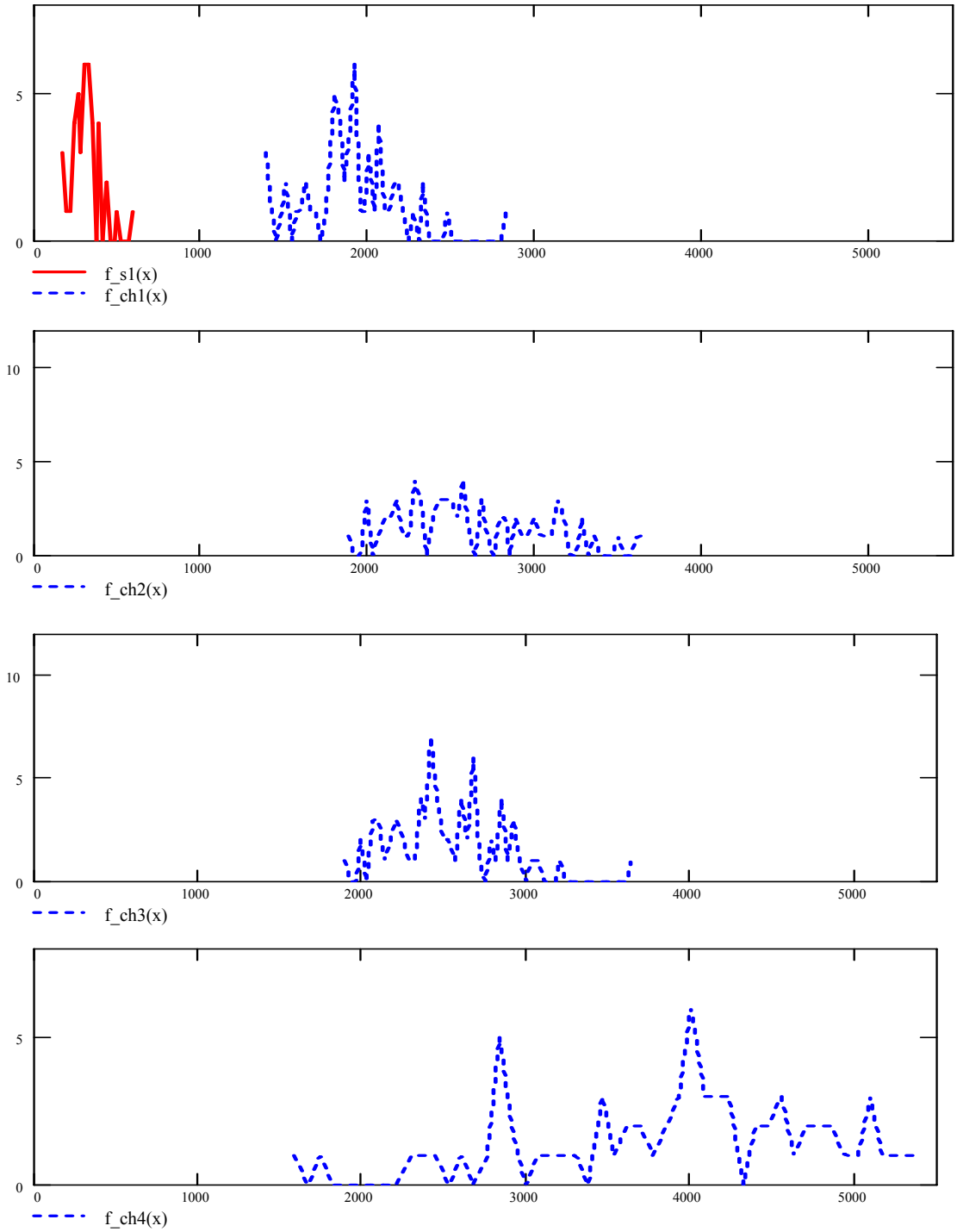


Рисунок 4.

На основании выше приведенных распределений можно сделать вывод, о том, что отсутствие сведений о зоне съема фонических сигналов не позволяет идентифицироваться "Чужому". Это означает, что даже используя тот же самый речевой сигнал возбуждения, невозможно идентифицироваться, не зная скрытого тракта звукопередачи до зоны съема, что позволяет говорить о возможности использования этого скрытого тракта в качестве секрета.

В дальнейшем при развитии биометрической технологии идентификации человека по голосу, с использованием ларингофона, предполагается использование нейросети, для формирования дополнительного неявного эталона в виде нейровесов, получаемых на этапе ее обучения [3]. Использование нейросети

позволит упростить этап обучения, уменьшая в соответствии с требованиями число итераций этого этапа.

ЛИТЕРАТУРА:

1 Способ автоматической идентификации личности. /Бочкарев С.Л., Иванов А.И., Андрианов В.В., Бочкарев В.Л. Оськин В.А // Патент РФ № 98115720 от 17.08.98. Заявитель ПНИЭИ.

2 Болдырев С.Г. Инструментальные средства биометрической идентификации человека по фоническим сигналам. Кафедра «Информационная Безопасность Систем и Технологий». ПГУ. 2003 (дипломный проект) 152 с.

3 Иванов А.И. Нейросетевые технологии биометрической аутентификации пользователей открытых систем. Специальность - системный анализ, управление и обработка информации. Автореферат диссертации на соискание ученой степени доктора технических наук. Пенза 2002.

Материалы поступили 28.04.2003. Опубликовано в Internet 30.06.2003

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.11-13. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/003)

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ

Коршунов М.Е. Пензенский государственный университет

Рассмотрим некоторые наиболее важные принципы построения корпоративной сети или ее защищенного фрагмента. Прежде всего, это требование закрытости на уровне пользователей и информационных серверов корпорации. Локальный характер и функциональное назначение подобной сети обуславливает также необходимость высокой эффективности (по сравнению с Internet) ее функционирования (как правило, в таких сетях высока интенсивность документооборота), что требует централизации служб сетевого администрирования.

Главными отличительными особенностями корпоративной сети можно считать централизованное управление сетью связи и заданный уровень защищенности сети, который определяется конфиденциальностью информации, обрабатываемой в сети корпорации, и учитывает средства и каналы связи всех существующих подсетей. Как правило, при построении корпоративной сети нельзя забывать и о желании отдельных пользователей иметь доступ в Internet. А это влечет за собой требование поддержки протоколов Internet для служб передачи данных (уровни 1-3 OSI), т. е. IP.

Следует заметить, что сегодня уже нельзя игнорировать развитость и технологии Internet, прежде всего средств передачи данных. Поэтому практически во всех современных протоколах альтернативных сетевых технологий прописаны правила инкапсуляции IP-дейтаграмм. Компромиссное решение для создания корпоративной сети, имеющей выход в Internet, должно базироваться на двух основных принципах:

1. Обязательное использование закрытого протокола при установлении соединения клиент-сервер, в рамках которого между абонентами сети согласуются параметры защищенного взаимодействия по виртуальному каналу связи (например, необходимость шифрования информации при передаче, применения электронной подписи) и решается задача выбора требуемого виртуального канала (если их несколько);
2. Доступность открытых протоколов (команд telnet, Ftp и т. д.) для взаимодействия по защищенному виртуальному каналу после установления соединения.

В корпоративной ЛВС должно обеспечиваться физическое разделение (подключение к различным связным ресурсам) серверов и рабочих мест, т. е. необходима организация подсетей рабочих мест и серверов. Во всех функциональных подсистемах (подсетях серверов и рабочих мест) нужно реализовать протоколы TCP/IP (для удаленных рабочих мест IP-пакеты инкапсулируются в пакеты соответствующих подсетей), что дает возможность использования сервисов Internet в корпоративной сети. Для того чтобы оградить корпоративную сеть от несанкционированного доступа, требуется обеспечивать следующие мероприятия:

- протоколы верхних уровней (5-7 уровни OSI) должны быть закрыты и несовместимы с протоколами телекоммуникационных служб Internet при установлении соединения и открыты при обмене информацией;

- при установлении соединения необходима защита от возможной подмены алгоритма взаимодействия клиента с сервером;
- сервер Internet (коммуникационный сервер доступа к Internet) должен быть исключен из подсети функциональных серверов и иметь собственную группу рабочих станций, исключенных из подсети функциональных рабочих мест;
- для реализации взаимодействия через подсети нужно снабдить корпоративную сеть межсетевыми средствами защиты от несанкционированного доступа. Эти средства должны обеспечивать сокрытие структуры защищаемых объектов, в частности IP-адресов, поскольку их шифрование недопустимо при использовании средств коммутации сетей передачи данных общего пользования.

Для эффективного функционирования сети должны быть реализованы централизованно ее службы административного управления, перечень которых определяется архитектурой управления взаимодействием открытых систем. В этот перечень входят службы управления: эффективностью функционирования, конфигурацией и именами, учетными данными, при отказах и сбоях. Поэтому в структуру корпоративной сети нужно включать средства маршрутизации и коммутации, функционирующие под протоколами TCP/IP, которые удаленно управляются из единого центра управления сетью связи, ЦУСС. К сожалению, не представляется возможным влиять на маршрутизацию, осуществляемую внутри подсети, к которой подключаются удаленные пользователи (с точки зрения построения корпоративной сети считаем, что здесь используются виртуальные каналы, которые не могут маршрутизироваться из ЦУСС).

Для обеспечения высокого уровня защищенности служба административного управления безопасностью должна быть централизованной. В сети необходимо организовать выделенный центр управления безопасностью (ЦУБ), который занимается сбором информации обо всех зарегистрированных нарушениях, ее обработкой и анализом с целью удаленного управления всеми техническими средствами защиты информации.

Следует особо отметить следующее. Функции ЦУС и ЦУБ не должны быть совмещены на одном рабочем месте администратора сети (несмотря на то, что они являются службами сетевого управления). Требуется предусмотреть алгоритм взаимодействия между ними, поскольку не исключено, что решения, принимаемые администраторами для управления и защиты корпоративной сети в процессе ее функционирования, могут оказаться прямо противоположными.

Сетевые экраны

Межсетевые средства защиты можно разделить на открытые и корпоративные. Первые - это межсетевые экраны (МЭ), функционирующие на основе открытых протоколов Internet и предназначенные для подключения к сети корпорации открытых серверов Internet. Корпоративные МЭ позволяют организовать в корпоративной сети защищенное взаимодействие клиент-сервер с закрытыми серверами корпорации, в том числе по виртуальным каналам сетей общего пользования.

Корпоративные межсетевые средства защиты делятся на внутренние и внешние. При этом внешние МЭ (они работают на виртуальном канале парами: входной и выходной) решают задачу разграничения прав доступа к виртуальному каналу связи и согласования параметров его защищенности при взаимодействии клиент-сервер, а внутренние обеспечивают разграничение прав доступа к ресурсам информационного сервера.

Требования к элементам системы защиты корпоративной сети включают в себя требования к МЭ корпорации (внутреннему и внешнему) и системе контроля

за целостностью информационных ресурсов. Межсетевой экран корпорации должен поддерживать следующие функции:

1. работа с оригинальными протоколами взаимодействия на уровнях 5-7 OSI в фазе установления соединения;
2. сокрытие IP-адресов информационных серверов (IP-адрес имеет только сервер аутентификации);
3. многоэтапная идентификация и аутентификация всех сетевых элементов;
4. физическое отделение рабочих станций и серверов от каналов сети передачи данных общего назначения (деление на подсети);
5. согласование качества обслуживания между межсетевыми средствами защиты глобальной сети при установлении соединения;
6. разграничение прав доступа пользователей корпоративной сети к серверам по нескольким критериям;
7. контроль за целостностью ПО и данных, в частности баз данных безопасности, а также отслеживание прерывания такого контроля во время сеанса обмена данными;
8. регистрация всех событий, связанных с доступом к серверам корпорации.

На уровне взаимодействия клиент-сервер МЭ должен использовать (в дополнение к службам контроля за доступом, аутентификации одноуровневых объектов и доступа к источникам данных) технические средства защиты (программные либо аппаратно-программные), включающие в себя следующие службы безопасности [1]:

1. засекречивания соединения;
2. засекречивания выборочных полей и потока данных;
3. контроля за целостностью соединения и выборочных полей;
4. защиты от отказов с подтверждением отправления и доставки.

Важнейшим следствием применения рассмотренных принципов организации межсетевых средств защиты является возможность разграничения прав доступа к БД безопасности при администрировании средств защиты, а также мандатного принципа управления доступом к информации. Администратор безопасности может не иметь допуска к данным, обрабатываемым в корпоративной сети, т.е. ему предоставляется доступ только к служебной информации (например, к БД безопасности на МЭ, к маршрутным таблицам и т. д.), а не к собственно корпоративной.

Существенное требование к любому межсетевому средству защиты - отсутствие «закладок».).

ЛИТЕРАТУРА:

1. ISO/TC 97/SC 21 N1528 ISO/DP 7498/2. Information Processing Systems - OSI Reference Model - Part 2: Security Architecture

Материалы поступили 3.05.2003. Опубликовано в Internet 30.06.2003

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.14-18. Секция-3: Нормотивное, методологическое и методическое обеспечение информационной безопасности.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/004)

МЕТОД СТАТИСТИЧЕСКОГО ОБНАРУЖЕНИЯ ВОЗДЕЙСТВИЙ ИМИТОПОМЕХ

Орощук И. М., Воронов М.В. E-mail: oimscient@mail.primorye.ru
Тихоокеанский военно-морской институт имени С.О. Макарова

Проведенные теоретические исследования и практические эксперименты показывают, что при воздействии имитационных помех в момент передачи полезных сообщений в цифровых каналах с регулярными замираниями происходит изменение стохастических характеристик принимаемого сигнала (рис. 1) [1-3]:

$$w(E_S)=\frac{E_S}{\sigma_s^2}\exp\left(\frac{E_S^2}{2\sigma_s^2}\right);\qquad w(E_N)=\frac{E_N}{\sigma_n^2}\exp\left(\frac{E_N^2}{2\sigma_n^2}\right);$$

$$w(E_Z)=\frac{E_Z}{(\sigma_s^2+\sigma_n^2)}\exp\left(-\frac{E_Z^2}{2(\sigma_s^2+\sigma_n^2)}\right),$$

где E_S – амплитуда напря-женности поля полезного сигнала; σ_s – среднеквадратичное отклонение орто-гональных составляющих напряженности поля полезного сигнала; E_N – ам-плитуда напряженности поля имитопомехи; σ_n – среднеквадратичное откло-нение ортогональных составляющих напряженности поля имитопомехи; E_Z – амплитуда напряженности суммарного поля полезного и имитационного сигналов.

Данный факт позволяет осуществлять обнаружение имитоатаки, и при использовании ортогональных видов манипуляции, фильтрацию суммарного сигнала от имитационных помех.

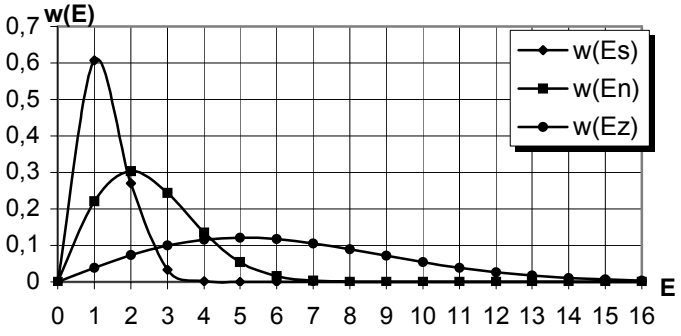


Рис. 1. Изменение плотности распределения при воздействии имитопомех

Сущность метода статистического обнаружения основана на обработке выборки данных принимаемого сигнала. Как показали исследования [1, 3], наиболее чувствительным является способ, основанный на оценке изменений статистики амплитуды. В качестве оценки предлагается использовать измерение математического ожидания (МО) стохастических флуктуаций амплитуды, вычисляемого как среднее арифметическое данных статистической выборки уровней принимаемого сигнала.

Для решения вопроса обнаружения возникает задача оценки изменений МО с определенной точностью и с заданной достоверностью, в противном случае задача лишается целесообразности. Согласно теореме Чебышева – Маркова [4]

точность оценки МО независимых и зависимых случайных величин определяется, прежде всего, объемом выборки:

$$P\left\{\left|\frac{1}{n}\sum_{r=1}^{n}\mu_r - \frac{1}{n}\sum_{r=1}^{n}M[\mu_r]\right| < \varepsilon\right\} > 1 - \frac{D[\overline{\mu}]}{\varepsilon^2}, \qquad (1)$$

где $M[\mu_r]$ – МО случайных нормированных амплитуд сигнала (в дальнейшем амплитуд) μ_r; $D[\overline{\mu}]$ – дисперсия среднего арифметического выборки случайных амплитуд; $D[\overline{\mu}] = D\left[\frac{1}{n}\sum_{r=1}^{n}\mu_r\right]$, ε – сколь угодно малая величина, определяющая требуемую точность оценки МО; n – объем выборки данных.

В общем случае, при наличии корреляционной связи между значениями выборки случайной функции значение дисперсии среднего арифметического определяется выражением

$$D[\overline{\mu}] = \frac{D_\mu}{n} + \frac{2}{n^2}\sum_{i<j}K_{i,j}, \qquad (2)$$

где D_μ – дисперсия случайной величины μ; $K_{i,j}$ – значение взаимной корреляции между двумя случайными значениями выборки μ_i и μ_j.

Из теоремы Маркова [4] известно, что значение $D[\overline{\mu}]$ должно снижаться по мере роста объема выборки. Однако для практической оценки МО возникает определенная сложность, которая заключается с одной стороны в ограниченности времени выборки из-за конечной длительности самого сеанса связи, и с другой стороны большим интервалом корреляции процесса замирания в реальных радиоканалах (рис. 2).

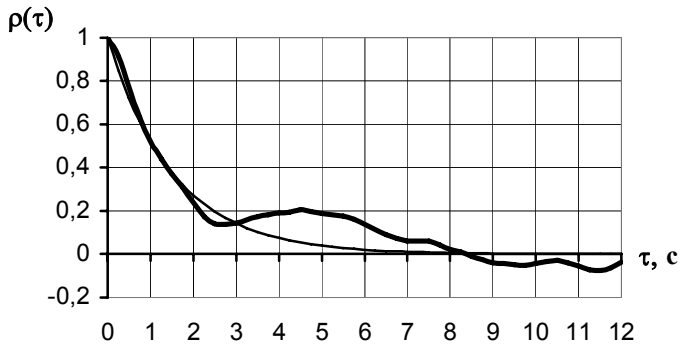


Рис. 2. Нормированная функция автокорреляции замираний в декаметровом

В результате, для оптимизации выборки необходимо решать компромисс, обеспечивающий максимальную точность при минимальной длительности выборки в масштабе времени. Кроме того, в решаемой задаче стоит вопрос выбора оптимального интервала сканирования, который определяет объем выборки, и, следовательно, требуемые характеристики оперативной памяти устройства измерения. Из соображений целесообразности, длительность наблюдения должна быть минимальной, исходя из чего функцию автокорреляции (см. рис. 2) можно рассматривать на ограниченном интервале времени, на котором приближенно ее можно аппроксимировать экспонентой. Данному приближению адекватна математическая модель канала с замираниями и группированием ошибок, которая основана на учете влияния динамических изменений уровня сигнала [5, 6].

Для оценки динамики замирания в предлагаемой модели процесс изменений уровня сигнала разделен относительно медианного значения $\mu_м$ на два состояния, в результате чего можно выделит моменты замирания и усиления

сигнала (рис. 3). В момент замирания уровень сигнал ниже среднего, а в момент усиления выше него.

Для упрощения модели с некоторым приближением на интервале замирания

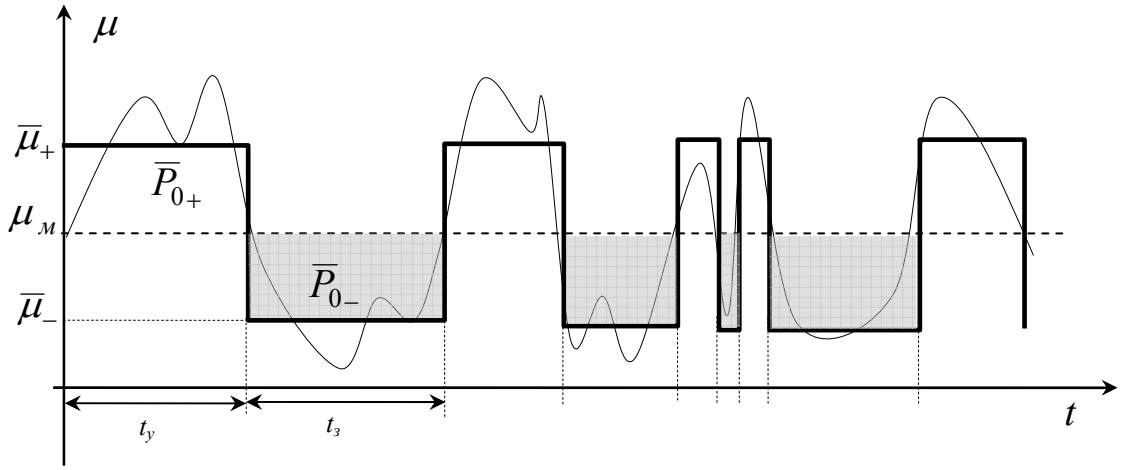


Рис. 3. Пояснение к динамической модели замираний

и усиления предлагается использовать средние значения коэффициента передачи эфира (см. рис. 3), величины которых для адекватности получим из известных значений числовых характеристик Рэлеевского распределения:

$$\begin{cases} \overline{\mu}_0 = \dfrac{\overline{\mu}_-}{2} + \dfrac{\overline{\mu}_+}{2} = \sigma_\mu \sqrt{\dfrac{\pi}{2}}; \\ \overline{\mu_0^2} = \dfrac{\overline{\mu_-^2}}{2} + \dfrac{\overline{\mu_+^2}}{2} = 2\sigma_\mu. \end{cases} \qquad (3)$$

Из решения системы уравнений (3) получим значения средних уровней на интервалах замирания – $\overline{\mu}_-$ и усиления – $\overline{\mu}_+$:

$$\overline{\mu}_{\mp} = \sigma_\mu \left[\sqrt{\frac{\pi}{2}} \mp \sqrt{2 - \frac{\pi}{2}} \right],$$

из которого $\overline{\mu}_- = 0{,}598\sigma_\mu$, $\overline{\mu}_+ = 1{,}908\sigma_\mu$.

На основании полученных значений коэффициентов передачи можно определить соответствующие вероятности ошибки приема бита (элемента) информации ($\overline{P}_{0-}$ – на участке замирания сигнала, $\overline{P}_{0+}$ – на участке усиления сигнала) [7].

Анализ статистики замираний [8] показал, что длительности замирания и усиления распределены по экспоненциальному закону (рис. 4):

$f(t) = \lambda_з e^{-\lambda_з t}$, где $\lambda_з = \dfrac{1}{\bar{t}_{з(у)}}$, $\bar{t}_{з(у)}$ – средняя длительность замирания или усиления сигнала.

В результате, при экспоненциальном распределении длительности

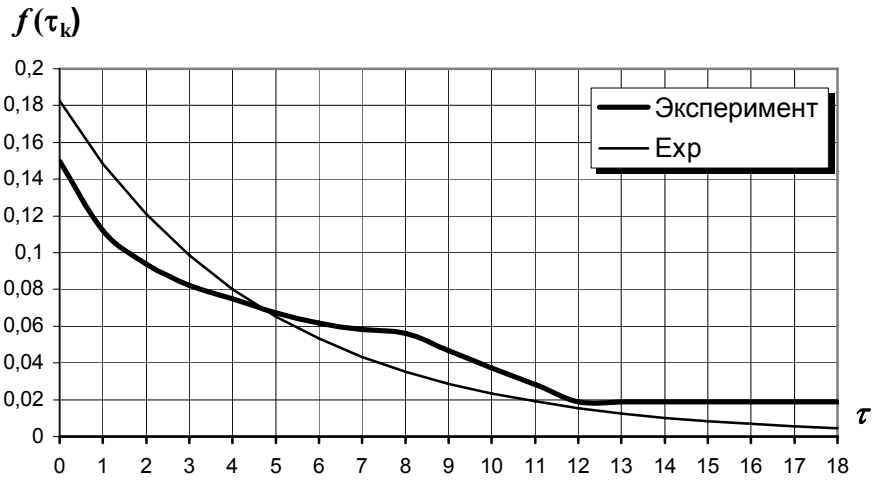


Рис. 4. Статистика длительности замираний

замираний моменты перехода канала в каждое состояние (замирания или усиления) представляют простейший пуассоновский поток [4]. Учитывая, что медианное значение уровня сигнала разделяет уровень на два равновероятных состояния, процесс перехода в одно из состояний представляет поток Эрланга второго порядка по отношению к общему потоку переходов в любое состояние (рис. 5).

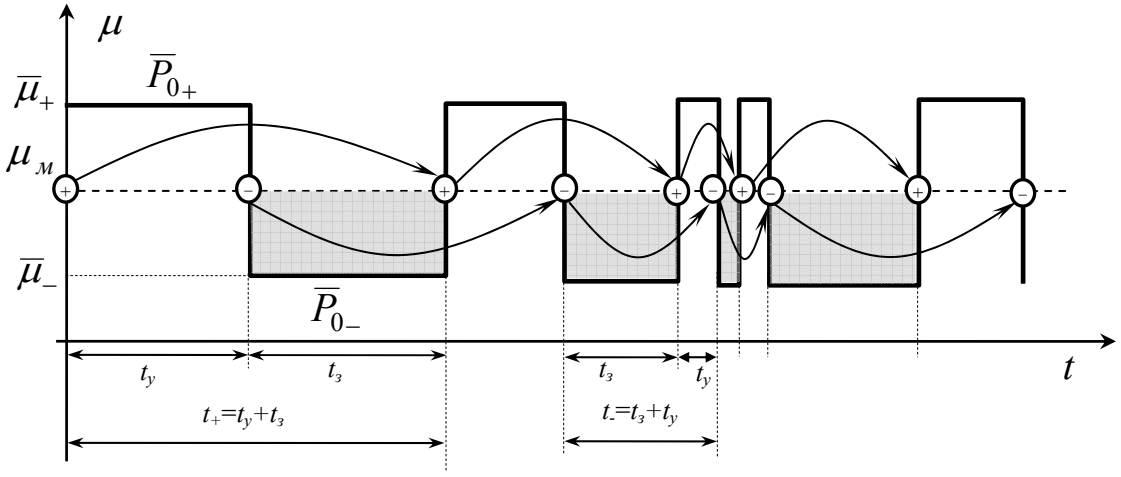


Рис. 5. Пояснение процесса замираний

В данном случае интенсивность переходов в определенное состояние (см. рис. 5) определяется выражением [4]

$$\lambda_+ = \lambda_- = \frac{1}{\bar{t}_з + \bar{t}_y} = \frac{\lambda_з}{2}. \qquad (4)$$

В результате действия этих потоков канал переходит в одно из двух состояний: ***«З»*** – замирания или ***«У»*** – усиления (рис. 6). При указанных потоках данная ситема состояний канала описывается Марковской моделью [4]. Оба

состояния канала составляют полную группу событий, в связи с чем

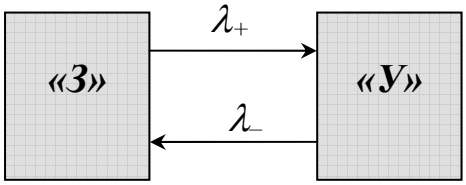


Рис. 6. Граф состояний канала связи

нормировочное условие будет определяться выражением $p_з + p_y = 1$.

Для определения вероятностей состояния модели составляется система линейных дифференциальных уравнений Колмогорова. Решение системы позволяет вычислить параметры модели, опираясь на ряд особых точек. Подробное решение системы дано в электронной версии работы (http://beda.stup.ac.ru/RV-conf/v04/004).

ЛИТЕРАТУРА**:**

1. Орощук И.М. Статистические изменения в радиоканале с регулярными замираниями при воздействии имитопомех // Научно-техническая конференция: "Безопасность информационных технологий", Сборник докладов. - Пенза, ПГУ, 2002. - Том 3. Секция 6. – С. 76-80.
2. Орощук И.М. Метод обнаружения и фильтрации имитационных помех в Рэлеевских каналах с замираниями // Безопасность информационных технологий: Москва, МИФИ. – № 3. – 2002. – С. 75-79.
3. Oroshchuk I. The statistical detection method of unauthorized intrusions in the Rayleigh fading channel //1st IEEE International Conference on Circuits and Systems for Communications. Proceedings. St. Petersburg, – 2002. – pp. 424-427. (на английском).
4. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. М.: Наука, 1991. – 384 с.
5. Орощук И.М. Динамическая модель Рэлеевского канала с замираниями // Журнал радиоэлектроники: М.: № 10. - 2002.
6. Орощук И.М. Метод и оценка эффективности статистического обнаружения воздействий имитопомех // Безопасность информационных технологий: Москва, МИФИ. – № 4. – 2002. – С. 87-92.
7. Зюко А.Г. Помехоустойчивость и эффективность систем связи. М.: Связь, 1972. – 360 с.
8. **До**луханов М.П. Флуктуационные процессы при распространении радиоволн. М.: Связь, 1971. – 184 с.
9. Головин О.В. Декаметровая радиосвязь. М.: Радио и связь, 1990. – 240 с.

Материалы поступили 5.05.2003. Опубликовано в Internet 30.06.2003

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.19-21. Секция-8: Конфиденциальность, целостность, доступность.
Пенза - 2003 (http://beda.stup.ac.ru/RV-conf/v04/005)

ТЕКСТОВАЯ СТЕГАНОГРАФИЯ

Д.В. Карташов, Г.Н. Чижухин

Цифровая компьютерная стеганография как наука родилась буквально в последние годы. По мнению специалистов [1] она включает следующие направления:

1) встраивание информации с целью ее скрытой передачи;
2) встраивание цифровых водяных знаков (watermarking);
3) встраивание идентификационных номеров (fingerprinting);
4) встраивание заголовков (captioning).

Если давать определение, то под *компьютерной цифровой стеганографией* следует понимать, в самом общем смысле (используя еще не устоявшуюся терминологию) - *науку о незаметном и надежном скрытии одних битовых последовательностей в других,* которые имеют избыточность. При этом имеющие избыточность совершенно не обязательно должны иметь аналоговую природу. Таким образом, целью стеганографии является сокрытие самого факта передачи информации.

По аналогии с криптографией, основным принципом стеганографии является предположение о том, что нарушитель знает распределение всех переменных в стегосистеме и само описание стегосистемы, но не знает используемого секретного ключа. Причем в отличие от криптографических, основной целью используемого ключа в стегосистемах является обеспечение неопределенности для нарушителя распределения скрываемого сообщения в контейнере. Кроме того, в стеганографии имеет место еще один принцип безопасности (назовем его стеганографический) – злоумышленник, наблюдая за обменом информации между отправителем и получателем, не должен обнаружить в ней передаваемую скрываемую информацию.

В данной работе основное внимание уделено стегосистемам первого направления, причем системам так называемой текстовой стеганографии, которое основано на использовании специальных свойств компьютерных форматов представления данных.

Направление текстовой стеганографии, связанное со скрытой передачей информации, сегодня уже нашло свое отражение в создании нескольких отработанных лицензионных программных продуктов.

На *I этапе* нашей работы были исследованы возможности пакета стеганографических программ FFENCODE (ОС DOS). Данный пакет представляет собой совокупность 2 программ: FFEncode (кодер стегосистемы) и FFDecode (декодер). Он свободно распространяется в Internete и обладает простым и понятным интерфейсом. Мы считаем, что этот пакет в своей основе использует один из методов компьютерной текстовой стеганографии: специальные свойства форматирования текстовых файлов (использование известного смещения слов, предложений, абзацев).

В результате проведенного эксперимента были получены следующие результаты:

1) стегоканал не обнаруживается визуально и его можно определить только при сравнении объема контейнера V_0, свободного от скрываемой

информации, с объемом заполненного контейнера V_3+о (так как V_3+о > V_o), если заранее известен V_0;

2) сжатие методами стандартного архивирования (RAR, ZIP и.т.д.) заполненного контейнера не приводит к искажению скрываемой информации;

3) в качестве контейнера целесообразно использовать только набор текстовых символов без каких-либо математических знаков, выражений, графиков. Любое отклонение от этого требования приводит к появлению ошибок при декодировании, а в конечном счете – к пропаданию стегоканала (если доля текстовых символов в общем объеме контейнера составляет менее 60 %). Это подтверждает наше предположение в отношении используемого метода встраивания скрываемой информации;

4) ограничений по использованию встраиваемого сообщения обнаружено не было (в качестве такого были использованы текстовый файл, звуковой файл формата MP3, видеосигнал формата MPEG4, графическое изображение, сжатое алгоритмом сжатия JPEG). Причем, объем встраиваемого сообщения превышал объем пустого контейнера в сотни (!) раз. Однако налицо демаскирующий признак – объем получаемого в результате стего превышал объем контейнера в десятки сотен (!) раз.

Таким образом, возникают следующие проблемы защиты передаваемой скрытно с помощью подобной цифровой стегосистемы информации: 1) если V_o не известен, то система обладает стегостойкостью и защита ее будет выливаться в достаточно сложные (и может даже невозможные методы стегоанализа); 2) если V_0 известен или получен из каких-то других источников, то можно предположить, что стегоканал можно определить уже при объемах информации, определяемых соотношением V_3+о/Vo - 1 > 0,2; 3) тогда для защиты необходимо как-то прятать стегоключ, который обеспечивает выделение из объема заполненного контейнера V_3+о скрываемого сообщения $У_с = V_{з+о} - V_o$; 4) в случае большой вероятности обнаружения стегоключа, необходимо шифровать само скрываемое сообщение, что к тому же будет подтверждать подлинность скрытно передаваемой информации.

II этап. На этом этапе была проведена передача стего по сети Internet с использованием средств электронной почты. Отметим, что передача стего от отправителя к получателю прошла успешно (администратор сети не обнаружил никаких признаков наличия стегоканала). Однако было получено еще одно ограничение при использовании данного пакета: декодирование на приемном конце происходит без ошибок только при сжатии стего стандартными архиваторами. В противном случае происходит преобразование текстового формата стего (.txt) в формат HTML и при обратном преобразовании перед декодированием происходит потеря (до 30%) скрываемого сообщения.

Все полученные результаты хорошо согласуются с теоретическими изысками по данному вопросу. Игнорирование характеристик контейнера существенно снижает скорость надежной передачи скрываемой информации. При заданных величинах искажений D_1 и D_2 (искажение кодирования и искажение, вносимое активным нарушителем, соответственно) игнорирование характеристик контейнера приводит к уменьшению величины пропускной способности (ПС) стегоканала в десятки раз (соответственно к увеличению ошибок при декодировании). В литературе [1] доказывается, что при использовании в качестве контейнера видео или речи, характеристики которых распределены не по нормальному закону при малых величинах D_1 и D_2 (большинство случаев на практике) величина скрытой ПС практически не уменьшается, а вот

использование контейнера с гауссовским распределением (которым, с небольшими допущениями, можно считать текстовое сообщение после сжатия его архиватором) сильно влияет на величину ПС.

Вообще, для класса информационно-скрывающих систем максимизируется скрытая ПС при обеспечении требуемой необнаруживаемости стегоканала, а к помехоустойчивости предъявляются минимальные требования.

В ряде работ скрытая связь (стеганография) рассматривается как передача скрываемых сообщений по каналу с помехами (в качестве помехи – контейнерный сигнал). Это позволяет свести задачу передачи скрываемых сообщений к хорошо исследованной задаче передачи открытых сообщений по обычному каналу с помехами. Для увеличения ПС в этом случае целесообразно увеличивать отношение сигнал/шум. Однако, с другой стороны, его надо ограничивать для обеспечения необнаруживаемости стегоканала.

Во многих практических стегосистемах скрываемое сообщение до встраивания шифруется или сжимается каким-либо архиватором (как и в нашем случае). Это увеличивает скрытность связи и позволяет описывать сжатое сообщение в виде последовательности с независимыми и равновероятными битами (гауссовский канал).

Таким образом, на данном этапе можно сделать следующие выводы.

1. Задача синтеза стегосистемы может быть сформулирована как задача поиска компромисса между ее характеристиками, так как улучшение одного ее параметра, например величины скрытой ПС, приходится обеспечивать за счет других параметров, таких, как скрытность передачи информации или устойчивость к разрушающему воздействию.

2. При образовании стегоканала внутри открытого канала передачи информации основной ресурс этого канала расходуется не на передачу скрываемого сообщения, а на передачу контейнера, выступающего в роли сигнала прикрытия скрываемого сообщения.

ЛИТЕРАТУРА:

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 272с.

2. Аграновский А.В., Балакин А.В. Стеганография в тексте. Труды НТК «Безопасность информационных технологий», том 2. – Пенза, 2001, с. 15-16.

3. FFENCODE. // http:// www.rugeley.demon.co.uk./security/ffencode.zip

Материалы поступили 10.05.2003. Опубликовано в Internet 30.06.2003

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.22-23. Секция-4: Анализ вычислительной среды, верификация, сертификация программ.
Пенза -2003 (http://beda.stup.ac.ru/RV-conf/v04/006)

СИНТЕЗ ЦИФРОВЫХ ЭЛЕКТРИЧЕСКИХ СХЕМ С ПОНИЖЕННЫМ РИСКОМ СБОЕВ

Кулагин О.В.
Пензенский научно-исследовательский электротехнический институт

Алгоритм работы, закладываемый в электрическую схему, может быть полностью искажен в процессе ее синтеза за счет рисков сбоев, возникающих в случае наличия в полученной схеме гонок или недопустимо больших задержек распространения сигналов. Для выявления рисков сбоев создано множество методов динамического анализа (моделирования) цифровых схем, но все они требуют явного указания входных тестовых наборов для моделируемой схемы [1-3]. Поэтому, желателен другой способ анализа и проектирования схем (особенно схем, синтезированных на основе алгебраических уравнений), позволяющий не формировать тестовые наборы. Назовем этот способ *алгоритмическим*. При нем необходимо принять меры к тому, чтобы в синтезируемой схеме не возникли риски сбоя, которые фактически искажают алгоритм, выполняемый схемой. Это может быть сделано за счет определения величин максимально допустимых временных задержек в схеме, гарантирующие отсутствие в ней рисков сбоев. Но сначала необходимо рассмотреть основные классы цифровых схем.

Их два – синхронные и асинхронные. Асинхронные схемы работают в непрерывном времени, т.е. они способны воспринимать входные сигналы и формировать соответствующие им выходные сигналы во всякий момент времени. Моделирование таких схем – процесс довольно сложный, требующий использования специального математического аппарата – непрерывной логики [4]. Синхронные схемы наоборот, работают в дискретном времени, задаваемом специальным сигналом, называемым синхросигналом или тактовой частотой. Такие схемы воспринимают входные сигналы только в отдельные моменты времени, между которыми в схеме сначала возникают переходные процессы, связанные с изменением входных сигналов, а по их окончании формируются истинные значения выходных сигналов, и затем схема простаивает. Следовательно, если обеспечить возможность окончания переходных процессов в схеме за время $(T-\tau)$, где T – период тактовой частоты, а $\tau<T/2$ – некоторый интервал времени, необходимый для гарантии появления истинных значений выходных сигналов схемы к моменту ее переключения, то синхронная схема будет работать без сбоев. Асинхронными элементами являются все виды комбинаторных логических элементов и асинхронные триггеры (например RS-триггеры), синхронными – синхронизируемые триггеры, защелки, регистры хранения, ОЗУ, ПЗУ и формирователи третьего состояния. Остальные электрические элементы, например счетчики, сдвиговые регистры, являются

комбинациями регистров хранения и комбинаторных узлов, т.е. они фактически являются схемами, а не элементами. Схема является синхронной в том случае, если в ней имеется хотя бы один синхронный элемент. В противном случае она будет асинхронной.

Любая синхронная схема может быть разделена на регистры хранения и асинхронные узлы. Для каждого такого узла необходимо определить величину максимальной задержки распространения сигнала t_{max}, по истечение которого в нем устанавливаются требуемые значения выходных сигналов. После определения величин t_{max} для всех асинхронных узлов схемы необходимо выбрать из них наибольшую величину, обозначим ее T_{max}, и на ее основе подсчитать период тактовой частоты T всей схемы по формуле, гарантирующей отсутствие рисков сбоев в синтезируемой схеме согласно следующему выражению

$$T \geq T_{max}+\tau \qquad (1)$$

Таким образом, алгоритмический контроль синтезируемой схемы позволяет исключить из процесса разработки схем общепринятое моделирование с использованием тестовых наборов.

ЛИТЕРАТУРА.

1. Воробьев Н. Риски сбоя в комбинационных схемах. // ChipNews, 1998, № 2. – с. 26-30.
2. Воробьев Н. Методы анализа комбинационных схем на риски сбоя. // ChipNews, 1998, № 3. – с. 42-44.
3. Воробьев Н. Рекомендации по устранению рисков сбоя в комбинационных схемах. // ChipNews, 1998, № 4. – с. 47-49.
4. Левин В.И. Динамика логических устройств и систем. – М.: Энергия, 1980.

Материалы поступили 20.05.2003. Опубликовано в Internet 30.06.2003

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.24-29. Секция-7: Аудит информационной безопасности
Пенза 2003 (http://beda.stup.ac.ru/RV-conf/v04/007)

АНАЛИЗ ПРОТОКОЛА АУТЕНТИФИКАЦИИ

Давыдов А.Н.

НПФ «Кристалл»

Основные положения BAN-логики

В BAN-логике различаются различные объекты: пользователи, ключи шифрования и формулы (также названные утверждениями). Символы A, B, и S обозначают пользователей; K_{ab}, K_{as} и K_{bs} обозначают общие ключи. Символы P, Q и R обозначают дополнительных пользователей; X и Y обозначают дополнительные утверждения; K обозначает ключи шифрования. Единственная пропозициональная связка является конъюнкцией и обозначается запятой. В BAN-логике используются следующие конструкции:

$P \models X$: P доверяет утверждению X; данная конструкция является основой для логики.

$P \triangleleft X$: P принял утверждение X. Некто послал сообщение, содержащее утверждение X, пользователю P; пользователь P может прочитать и повторить утверждение X (возможно после выполнения расшифрования).

$P \mid\sim X$: P однажды заявил утверждение X; пользователь P когда-то послал сообщение, включающее утверждение X; не известно, когда было послано сообщение: давно или в течение работы протокола, но известно, что пользователь P верил утверждению X, когда посылал сообщение.

$P \Rightarrow X$: P обладает полномочиями над X; пользователь P является автором утверждения X; эта конструкция используется, когда пользователь имеет права на создание некоторых утверждений. Например, ключи шифрования должны генерироваться с особым вниманием, и в некоторых протоколах данную операцию выполняют доверенные серверы. Это может выражаться предположением, которому пользователи верят, что сервер имеет полномочия над утверждениями о качестве ключей.

#(X): утверждение X является свежим; под термином «свежий» понимается, что утверждение X не было послано до начала работы протокола.

$P \xleftrightarrow{K} Q$: пользователи P и Q могут использовать общий ключ K для установки связи; ключ K известен только пользователям P и Q или другим пользователям, которым P или Q доверяют; другим пользователям ключ K не известен.

$P \overset{X}{\Longleftrightarrow} Q$: утверждение X является секретом, известным только пользователям P и Q и, возможно, пользователям, которым они доверяют; только P и Q могут использовать X для доказательства своей идентичности один другому; примером является пароль.

$\{X\}_K$: шифротекст от X на ключе K.

$\langle X \rangle_Y$: объединение (конкатенация) утверждения X и секрета Y; секрет Y полностью идентифицирует объект, заявивший утверждение X; в реализациях утверждение X, как правило, просто конкатенируется с паролем Y.

Постулаты BAN-логики

При анализе протоколов аутентификации следует различать два времени: прошлое и настоящее. Настоящее время начинается на старте работы изучаемого протокола. Все убеждения, имеющие место в настоящем, являются неизменными до завершения выполнения протокола; кроме того, допускается, что когда пользователь P заявляет X, то он действительно доверяет X.

Зашифрованное сообщение представляется как логическое утверждение, зашифрованное на ключе шифрования. Шифрованное сообщение не может быть расшифровано пользователем, не имеющим ключа. Ключ не может быть получен из шифрованного сообщения. Каждое шифрованное сообщение содержит избыточность достаточную, чтобы пользователь, расшифровывающий данное сообщение, имел возможность проверить, что он использовал правильный ключ. Кроме того, сообщения содержат информацию, необходимую пользователю, чтобы обнаружить и проигнорировать его собственные сообщения.

Правила значения сообщения имеют отношение к интерпретации сообщений. Два первых правила позволяют интерпретировать шифрованные сообщения, а третье правило позволяет интерпретировать сообщения с секретами. Они все объясняют процесс получения доверия о происхождении сообщений.

Для общих ключей формула выглядит следующим образом:

$$\frac{P \models Q \overset{K}{\longleftrightarrow} P,\ P \triangleleft \{X\}_K}{P \models Q \mid\sim X}.$$

Если пользователь P верит, что ключ K есть только у него и Q, и получает сообщение X, шифрованное на ключе K, то P верит, что это Q прислал сообщение X. Чтобы данное правило имело смысл, необходимо гарантировать, что пользователь P не послал сообщение X сам себе.

Для общих секретов формула выглядит следующим образом:

$$\frac{P \models Q \overset{Y}{\Leftrightarrow} P,\ P \triangleleft \langle X \rangle_Y}{P \models Q \mid\sim X}.$$

Если пользователь P верит, что секрет Y есть только у него и у пользователя Q, и получает $\langle X \rangle_Y$, то P верит, что это пользователь Q прислал X.

Правило проверки нонсов:

$$\frac{P \models \#(X),\ P \models Q \mid\sim X}{P \models Q \models X}.$$

Если пользователь P верит, что сообщение X является свежим и что его отправил пользователь Q, то P верит, что Q доверяет X. Для простоты, X должно быть открытым текстом и не должно включать никаких шифрованных подстрок.

Правило полномочий указывает, что если P верит, что Q создал утверждение X, и P доверяет Q, то P убеждён в истинности X:

$$\frac{P \models Q \Rightarrow X,\ P \models Q \models X}{P \models X}.$$

Неизбежным свойством оператора доверия является то, что пользователь P верит ряду утверждений тогда и только тогда, когда он верит каждому отдельному утверждению. Это обосновывает следующие правила:

$$\frac{P \models X,\ P \models Y}{P \models (X,Y)},\qquad \frac{P \models (X,Y)}{P \models X},\qquad \frac{P \models Q \models (X,Y)}{P \models Q \models X}.$$

Другие аналогичные правила могут быть введены при необходимости.

Если пользователь получает сообщение, то он также получает все поля данного сообщения, если он знает необходимые ключи:

$$\frac{P \lhd (X,Y)}{P \lhd X}, \qquad \frac{P \lhd \langle X \rangle_Y}{P \lhd X}, \qquad \frac{P \models Q \xleftrightarrow{K} P,\ P \lhd \{X\}_K}{P \lhd X},$$

Предполагается, что пользователь P не послал сообщение X сам себе.

Если одна часть формулы является свежей, то целая формула тоже является свежей:

$$\frac{P \models \#(X)}{P \models \#(X,Y)}.$$

Можно написать и другие аналогичные правила. Например, можно показать, что если утверждение X является свежим, то $\{X\}_K$ также является свежим.

Для добавления понятия «хэш-функция» в BAN-логику вводится символ H для представления хэш-функций. Правило получения атрибутов авторства сообщения X из сообщения H(X) будет следующим:

$$\frac{P \models Q \mid\sim H(X_1,...,X_k),\ P \lhd X_1,...,P \lhd X_k}{P \models Q \mid\sim (X_1,...,X_k)}.$$

Анализ протоколов

Анализ протокола выполняется следующим образом:

1. Получение идеализированного протокола, производного от подлинника.
2. Написание предположений о начальном состоянии.
3. Добавление логических формул к утверждениям протокола, как суждений о состоянии системы после каждого утверждения.
4. Логические постулаты используют суждения и утверждения для обнаружения убеждений, полученных сторонами в ходе выполнения протокола.

Анализ протокола аутентификации участников сеанса

Описание протокола аутентификации

Описываемый протокол позволяет двум субъектам A и B аутентифицировать друг друга на основе общего секретного ключа аутентификации (СКА) и цифровых идентификаторов (DI_a и DI_b). До выполнения протокола участники должны знать значения цифровых идентификаторов друг друга и выработать общий секретный ключ аутентификации. Каждый субъект протокола должен иметь датчик случайных чисел для генерации нонсов, синхронизированные часы и алгоритм вычисления хэш-функции с ключом (H). Для защиты от атак повтора сообщений используются случайные последовательности – нонсы (N_a и N_b). Отметка времени T_a необходима для проверки приемлемости первого сообщения протокола. Символ ‖ в описании протокола означает операцию конкатенации.

1. Объект A:

- генерирует нонс N_a;
- считывает с системных часов отметку времени T_a;
- вычисляет $h_a = H_{СКА}(B \| A \| T_a \| DI_a \| N_a)$;
- посылает B сообщение $[B \| A \| T_a \| N_a \| h_a]$.

2. Объект B:

- получает от A сообщение $[B \| A \| T_a \| N_a \| h_a]$;
- считывает отметку времени t_b;
- проверяет условие $|t_b - T_a| < \Delta$;
- получает из базы данных цифровой идентификатор объекта A – DI_a;
- проверяет условие $h_a \overset{?}{=} H_{СКА}(B \| A \| T_a \| DI_a \| N_a)$;
- если хотя бы одно из условий не выполняется, протокол разрывается; при выполнении этих условий B аутентифицирует A;

- генерирует нонс N_b;
- вычисляет $h_b = H_{CKA}(A \| B \| DI_b \| N_a \| N_b)$;
- посылает A сообщение $[A \| B \| N_a \| N_b \| h_b]$.

3. Объект A:

- получает от B сообщение $[A \| B \| N_a \| N_b \| h_b]$;
- сравнивает полученное значение нонса N_a с переданным;
- получает из базы данных цифровой идентификатор объекта B – DI_b;
- проверяет условие $h_b \overset{?}{=} H_{CKA}(A \| B \| DI_b \| N_a \| N_b)$;
- если хотя бы одно из этих условий не выполняется, протокол разрывается; в случае выполнения этих условий A аутентифицирует B и узнаёт, что B аутентифицировал A;
- вычисляет $h_{a2} = H_{CKA}(B \| A \| N_b \| N_a)$;
- посылает B сообщение $[B \| A \| N_b \| h_{a2}]$.

4. Объект B:

- получает от A сообщение $[B \| A \| N_b \| h_{a2}]$;
- сравнивает полученное значение нонса N_b с переданным;
- проверяет условие $h_{a2} \overset{?}{=} H_{CKA}(B \| A \| N_b \| N_a)$;
- если хотя бы одно из этих условий не выполняется, протокол разрывается; в случае выполнения этих условий B узнаёт, что A аутентифицировал B.

Идеализация протокола

В идеализированной форме опускается часть сообщения, не относящаяся к доверию. Удаляются указатели, которые добавлены к реализации для своевременного выполнения процедур, но чье присутствие не затрагивает результата протокола, если каждый приёмник действует самопроизвольно. Например, можно опустить сообщение, использованное в качестве стартовой посылки, запускающей сеанс связи. Открытый текст опускается просто потому, что он может быть подделан.

Сообщение 1 A → B: $T_a, N_a, \langle H(T_a, N_a) \rangle_{DI_a, CKA}$;

Сообщение 2 B → A: $N_a, N_b, \langle H(N_a, N_b) \rangle_{DI_b, CKA}$;

Сообщение 3 A → B: $N_b, \langle H(N_b, N_a) \rangle_{CKA}$.

Предложения

Для анализа протокола следует сделать следующие предположения.

$A \models A \overset{CKA}{\Leftrightarrow} B$; $B \models A \overset{CKA}{\Leftrightarrow} B$;

$A \models A \overset{DI_A}{\Leftrightarrow} B$; $B \models A \overset{DI_B}{\Leftrightarrow} B$;

$A \models A \overset{DI_B}{\Leftrightarrow} B$; $B \models A \overset{DI_A}{\Leftrightarrow} B$;

$A \models B \Rightarrow N_b$; $B \models A \Rightarrow N_a$;

$A \models \#N_a$; $B \models \#N_b$;

$B \models \#T_a$.

Первые два предположения говорят о том, что объекты A и B доверяют общему ключу аутентификации СКА. Два следующих предположения описывают, что объекты A и B доверяют своим цифровым идентификаторам DI_a и DI_b соответственно. Следующие два предположения показывают, что объекты A и B доверяют цифровым идентификаторам других абонентов. Седьмое и восьмое предположения показывают, что объекты A и B сами генерируют свои нонсы.

Девятое и десятое предположения говорят о том, что объекты A и B верят в свежесть сгенерированных ими нонсов. Последнее предположение предполагает использование синхронизированных часов, так как каждый объект должен проверять свежесть меток времени, сгенерированных другим объектом.

Формальный анализ протокола

Объект B получает сообщение 1: $B \lhd T_a, N_a, \langle H(T_a, N_a) \rangle_{DI_a, CKA}$, откуда по формуле $\frac{P \lhd (X, Y)}{P \lhd X}$ получают:

$$B \lhd T_a, N_a; \qquad B \lhd \langle H(T_a, N_a) \rangle_{DI_a, CKA}.$$

Учитывая предположения $B \models A \overset{CKA}{\Leftrightarrow} B$ и $B \models A \overset{DI_A}{\Leftrightarrow} B$, по правилу значения сообщений для общих секретов получают:

$$B \models A \mid\sim H(T_a, N_a).$$

Откуда по правилу $\frac{P \models Q \mid\sim H(X_1, ..., X_k),\ P \lhd X_1, ..., P \lhd X_k}{P \models Q \mid\sim (X_1, ..., X_k)}$ получают:

$$B \models A \mid\sim T_a, N_a.$$

Используя полученный результат и предположение $B \models \#T_a$, по правилу проверки нонсов получают:

$$B \models A \models N_a.$$

Отсюда, используя правило полномочий и предположение $B \models A \Rightarrow N_a$, получают:

$$B \models N_a.$$

Таким образом, B аутентифицирует A.

Получив сообщение 2, A узнаёт, что $B \models N_a$, поэтому в идеализированном протоколе его следует изменить следующим образом:

$$A \lhd N_a, N_b, \langle H(N_a, N_b), B \models N_a \rangle_{DI_B CKA}.$$

Из сообщения 2 по формуле $\frac{P \lhd (X, Y)}{P \lhd X}$, получают:

$$A \lhd N_a, N_b; \qquad A \lhd \langle H(N_a, N_b), B \models N_a \rangle_{DI_B CKA}.$$

Учитывая предположения $A \models A \overset{CKA}{\Leftrightarrow} B$ и $A \models A \overset{DI_B}{\Leftrightarrow} B$, по правилу значения сообщений для общих секретов получают:

$$A \models B \mid\sim (H(N_a, N_b), B \models N_a).$$

Откуда по правилу $\frac{P \models Q \mid\sim H(X_1, ..., X_k),\ P \lhd X_1, ..., P \lhd X_k}{P \models Q \mid\sim (X_1, ..., X_k)}$. получают:

$$A \models B \mid\sim (N_a, N_b, B \models N_a).$$

Используя полученный результат и предположение $A \models \#N_a$, по правилу проверки нонсов получают:

$$A \models B \models N_b; \qquad A \models B \models N_a.$$

Из выражения $A \models B \models N_a$ и предположения $A \models B \Rightarrow N_b$ по правилу полномочий получают:

$$A \models N_b.$$

Последнее выражение фактически означает аутентификацию объекта B объектом A. Выражение $A \models B \models N_b$ означает, что объект A узнаёт, что объект B его аутентифицировал.

Получив сообщение 3, B узнаёт, что $A \models N_b$ поэтому сообщение 3 в идеализированном протоколе следует изменить следующим образом: $B \triangleleft N_b, \langle H(N_b, N_a), A \models N_b \rangle_{СКА}$.

Из сообщения 3 по формуле $\frac{P \triangleleft (X,Y)}{P \triangleleft X}$, получают:

$$A \triangleleft N_b; \qquad B \triangleleft \langle H(N_b, N_a), A \models N_b \rangle_{СКА}.$$

Учитывая предположение $A \models A \overset{СКА}{\Leftrightarrow} B$, по правилу значения сообщений для общих секретов получают:

$$B \models A \mid\sim (H(N_b, N_a), A \models N_b).$$

Откуда по правилу $\frac{P \models Q \mid\sim H(X_1,...,X_k),\ P \triangleleft X_1,...,P \triangleleft X_k}{P \models Q \mid\sim (X_1,...,X_k)}$ получают:

$$B \models A \mid\sim (N_b, A \models N_b).$$

Используя полученный результат и предположение $B \models \#N_b$, по правилу проверки нонсов получают:

$$B \models A \models N_b.$$

Последнее выражение означает, что объект B узнаёт, что объект A его аутентифицировал.

Выводы

1. Проанализированный протокол аутентификации обеспечивает аутентификацию объекта B объектом A и аутентификацию объекта A объектом B в ходе выполнения протокола.

2. Протокол содержит некоторую избыточность. В своей работе он использует следующие общие секреты:
   - общий ключ аутентификации объектов – СКА;
   - цифровой идентификатор объекта A – DI_a;
   - цифровой идентификатор объекта B – DI_b.

Достаточно использовать лишь один из трёх перечисленных секретов. Использование одного секрета вместо трёх не ослабляет протокол, что можно показать с помощью логики. Значение хэш-функции в сообщении 3 вычисляется от нонсов N_a и N_b. Достаточно вычислять значение хэш-функции только от N_b, что можно показать с помощью логики.

Литература

1. Michael Burrows, Martin Abadi, Roger Needham. A Logic of Authentication. ACM Translations in Computer Systems, 8(1): 18-36, February 1990.

Получено 12.10.2003. Доклад опубликован в Internet 18.10.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С. 30- 36. Секция- 9: Аутентификация: парольная, биометрическая, криптографическая
Пенза-август-2003 (http://beda.stup.ac.ru/04v/008)

ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ РЕАЛИЗАЦИИ СХЕМЫ ЦИФРОВОЙ ПОДПИСИ ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ МОДУЛЯ СПЕЦИАЛЬНОГО ВИДА

Спиридонов А.В. E-mail: spx@mail15.com
Пензенский государственный университет

Введение

В последней четверти двадцатого столетия на стыке теории сложности алгоритмов, алгоритмической теории чисел и компьютерной алгебры зародилось и в наши дни переживает настоящий бум направление, известное как криптография с открытым ключом. Оно позволяет успешно решать разнообразные задачи, связанные с защитой информации в компьютерных сетях, в том числе задачу использования *электронной цифровой подписи* (ЭЦП).

В Российской Федерации до недавнего времени действовал стандарт на процедуры ЭЦП ГОСТ Р 34.10-94, использовавший (как и большинство иностранных алгоритмов) криптографическую технику, основанную на арифметике мультипликативной группы простого поля. Однако с 1 июля 2002 г. вступил в действие ГОСТ Р 34.10-2001, который в отличие от прежнего предлагает использовать криптографическую схему, основанную (что также является мировой тенденцией) на арифметике группы точек эллиптической кривой. Переход к эллиптической криптографии обусловлен теми преимуществами, которые дает её использование – меньшая длина ключа при заданной стойкости. Например, в построенных на основе эллиптических кривых криптосистемах бинарной размерности в диапазоне от 150 до 350 обеспечивается уровень криптографической стойкости, который требует использования в известных криптосистемах бинарной размерности от 600 до 1400 и более [1]. Кроме этого, несмотря на то, что операции в эллиптической криптографии сложнее (вычислительно), за счет меньшей длины операндов и выбора наиболее эффективных арифметических алгоритмов можно даже получить выигрыш в производительности по сравнению с процедурами ЭЦП на основе арифметики мультипликативной группы простого поля (при сохранении заданной криптографической стойкости).

В данной работе рассматриваются методы вычисления модулярной редукции (вычисление остатка от деления целых чисел на целое число – модуль) – одной из базовых элементарных криптографических операций. Эта довольно старая тема вызвала интерес в новом контексте по следующей причине: новый стандарт на ЭЦП открывает путь, ранее закрытый, – применение в качестве модуля чисел специального вида, вычисление редукции по которым можно реализовать весьма эффективно. ГОСТ 34.10-94 не позволял использовать в качестве модуля такие числа в силу четкого определения процедуры генерации используемых простых чисел. Новый ГОСТ 34.10-2001 не накладывает подобных ограничений. Особо следует отметить, что к настоящему времени неизвестно о каких-либо негативных последствиях использования такого числа в качестве параметра схемы ЭЦП (а именно как модуля кривой) по ГОСТ 34.10-2001.

Таким образом, данная работа посвящена исследованию чисел специального вида и соответствующих им алгоритмов вычисления редукции,

позволяющих повысить производительность вычислений процессов формирования/проверки ЭЦП на основе криптографии эллиптических кривых. В работе проводится сравнение данных алгоритмов с универсальными алгоритмами (не зависящими от вида модуля), а также производится оценка вклада перехода на модули специального вида в повышение общей производительности вычисления алгоритмов ГОСТ 34.10-2001.

Методы вычисления модулярной редукции

Модулярной редукцией или *редукцией по модулю натурального числа n* будем называть вычисление остатка от деления целых чисел на n.

В данной работе рассматриваются пять методов вычисления модулярной редукции (далее просто *редукция*):

- классический алгоритм деления длинных чисел;
- редукция Барретта;
- редукция Монтгомери;
- редукция по модулю чисел Кронделла;
- редукция по модулю обобщенных чисел Мерсенна.

Первые три являются универсальными, т.е. не зависят от вида модуля, два последних – требуют модуля специального вида. Как уже упоминалось выше, в действовавшем раннее ГОСТ Р 34.10-94 зафиксирована процедура генерации простого числа p, которая не позволяла получать числа специального вида, и соответственно, применение специальных методов было невозможно. ГОСТ Р 34.10-2001 ничего подобного не содержит, поэтому исследование методов вычисления редукции по модулю специального вида становится актуальным в контексте поиска решений по повышению производительности реализаций алгоритмов ГОСТ Р 34.10-2001.

Дополнительная терминология

Будем называть числа, двоичное представление которых имеет больше разрядов, чем штатно используется в ЭВМ для представления целого числа (обычно это 16, 32 или 64 бита), *длинными числами* (*числами повышенной разрядности*). Например, число длиной 256 бит определённо длинное число.

Обозначим через m длину машинного слова, а в качестве основания системы счисления примем $b = 2^m$. Как известно, любое неотрицательное целое число $X < b^n$ можно разложить в сумму степеней числа b:

$$X = X_0 b^0 + X_1 b^1 + \ldots + X_{n-2} b^{n-2} + X_{n-1} b^{n-1}$$

где X_i – некоторые неотрицательные целые числа меньшие b. Число X хранится в памяти компьютера как массив m-битовых слов с элементами $X[i] = X_i$. Будем называть числа X_i *цифрами* числа X, а число X – n-значным длинным числом.

Можно отождествить поле GF(p) с множеством целых неотрицательных чисел меньших p. Тогда элементы поля GF(p) можно представить как неотрицательные длинные целые числа меньшие p. Если обозначить через n количество цифр числа p, то элементы GF(p) в памяти компьютера представляются как массивы из n элементов-цифр.

Классический алгоритм деления длинных чисел

Для вычисления остатка можно тривиально воспользоваться классическим алгоритмом деления «лесенкой». Он широко известен, достаточно точно формализован (см., например, алгоритм 14.20 в [6]) и является одним из самых медленных вариантов вычисления редукции. Не будем на нём подробно останавливаться, отметим только, что при вычислении редукции числа длины $2n$

цифр по модулю числа длины n цифр с помощью деления требуется в среднем выполнение порядка n элементарных делений и $n(n + 2{,}5)$ умножений [3].

Редукция Барретта

Барретт предложил алгоритм, позволяющий вычислить $r = x \bmod p$ для данных x и p длиной k бит (частное в ходе вычислений не определяется). При этом алгоритм требует предварительного вычисления числа $\mu = \lfloor b^{2k} / p \rfloor$, что позволяет значительно упростить вычисления в дальнейшем. В частности в алгоритме отсутствуют «тяжелые» операции деления – остаются только деления на степень основания системы счисления, которые на практике реализуются «легкой» операцией сдвига. При однократном вычислении редукции по вычислительной сложности алгоритм Барретта близок к делению, однако при многократном вычислении редукции по одному и тому же модулю, что и наблюдается при вычислениях в группе, он оказывается гораздо эффективнее (ведь μ достаточно вычислить один раз!). В [3] показывается, что при вычислении редукции числа длины $2n$ цифр по модулю числа длины n цифр с помощью алгоритма Барретта требуется выполнить $n(n + 4)$ элементарных операций умножения. Сам алгоритм достаточно прост и приведен, например, в [6].

Редукция Монтгомери

Монтгомери [7] предложил пойти другим путём. Пусть p - натуральное число, T и R - целые числа, такие что

$$0 \le T < pR,$$
$$p < R,$$
$$\text{НОД}(p, R) = 1.$$ (НОД – наибольший общий делитель.)

Число $TR^{-1} \bmod p$ называется *редукцией Монтгомери* числа T по модулю p *относительно* R. При подходящем выборе R редукцию Монтгомери можно вычислить весьма эффективно.

Пусть x и y – целые числа: $0 \le x, y < p$. Пусть $x' = xR \bmod p$, $y' = yR \bmod p$. Тогда редукцией Монтгомери произведения $x'y'$ является $x'y'R^{-1} \bmod p = xyR \bmod p$. Именно это свойство позволяет использовать редукцию Монтгомери для эффективного вычисления модулярной экспоненты (что весьма кстати в процедурах ЭЦП).

Для вычисления значения редукции Монтгомери используется следующий факт.

Пусть $p' = -p^{-1} \bmod R$, $U = Tp' \bmod R$. Тогда число $(T+Up)/R$ целое и

$$(T+Up)/R \equiv TR^{-1} \pmod p.$$

Если представить число p в общем случае в b-ичной системе счисления, то удобно использовать $R = b^n$. Условие $p < R$ очевидно выполняется. Что же касается требования $\text{НОД}(p,R) = 1$, то оно равносильно $\text{НОД}(p,b) = 1$. Если b – степень 2, то последнее условие равносильно тому, что p – нечетное число. Для простых p, используемых в процедурах цифровой подписи, это верно. В [7] (а также в [3] и [6]) приводится алгоритм для вычисления редукции Монтгомери, причем в [3] показано, что он требует выполнения $n(n + 1)$ элементарных операций умножения и некоторого количества операций сложения.

Как видно, скорости вычисления редукции Монтгомери и Барретта довольно близки. И всё же редукция Монтгомери требует слегка меньшего количества операций и легче поддается распараллеливанию, поэтому она, как правило, и используется в реализациях ГОСТ Р 34.10-94.

Редукция по модулю обобщенных чисел Мерсенна

Вышеприведённые алгоритмы являлись универсальными, т.е. позволяли вычислить редукцию по произвольному простому модулю. Однако можно

выбрать модуль, для которого вычисление редукции выполняется особенно эффективно. Наиболее известным из таких чисел является число Мерсенна – число, в общем случае имеющее вид $p = 2^k - 1$. Для вычисления редукции $2k$-битного числа A по такому модулю следует представить его в виде

$$A = A_1 + 2^k A_2,$$

где $0 \le A_1, A_2 < 2^k$.

Тогда

$$A \equiv A_1 + A_2 \pmod{p}.$$

Как видно, редукция по модулю числа Мерсенна может быть выполнена без деления или умножения, а только с помощью сложения.

На практике было бы удобно, чтобы k было кратно длине машинного слова используемой ЭВМ (степень двойки), но в этом случае k – составное число и $p = 2^k - 1$ не простое. Следовательно, автоматическое использование упрощения редукции, предоставляемого числами Мерсенна, не применимо в контексте нашей задачи.

Однако можно расширить понятие чисел Мерсенна одним из следующих способов:

- числа Кронделла вида $p = b^n \pm c$, где $0 < c < b$ ([4]), длину b можно выбрать равной длине машинного слова;
- обобщенные числа Мерсенна вида $p = b^n - c_{n-1}b^{n-1} - \ldots - c_0$, где лишь малое число c_i не равны 0 ([8]).

Пусть модуль $p = b^n - c_{n-1}b^{n-1} - \ldots - c_0$, с большим количеством нулевых c_i. В [8] разработана техника вычисления редукции по таким модулям. При этом применяются регистры сдвига с линейной обратной связью.

В качестве примера, подходящего для случая ГОСТ Р 34.10-2001, рассмотрим простое число, предложенное в новой редакции американского стандарта цифровой подписи *ECDSA* [5] (там же указаны параметры кривой, построенной с его использованием). Это

$$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1.$$

В [5] приводятся формулы, позволяющие вычислить редукцию по этому модулю, выполнив в общей сложности всего 10 операций сложения, вычитания и сдвига 256-битных чисел с последующей редукцией по модулю p числа, которое превышает p на 0÷6 разрядов. Таким образом, в данном случае не требуется использовать ни операций деления, ни операций умножения. Все вычисления выполняются с помощью аддитивных операций. Соответственно, скорость такой редукции существенно выше всех ранее рассмотренных методов. Это же верно для многих обобщенных чисел Мерсенна с небольшой плотностью (см. [8]).

Редукция по модулю чисел Кронделла

Числами Кронделла называют простые числа вида $p = b^n \pm c$, где $0 < c < b$. Редукция по модулю таких чисел также может быть реализована более эффективно, чем для произвольных простых чисел.

Пусть $p = b^n - c$, где $0 < c < b$.Тогда

$$b^n \equiv c \pmod{p}.$$

Значит для числа $A = A_1 + b^n A_2$, где $0 \le A_1, A_2 < b^n$,

$$A \equiv A_1 + cA_2 \pmod{p}.$$

Следовательно, для вычисления редукции $2n$-значного числа по модулю n-значного числа Кронделла необходимо выполнить умножение n-значного числа на цифру, сложение $(n + 1)$-значного и n-значного чисел, и после этого вычислить редукцию $(n + 1)$-значного числа по n-значному модулю. Если на последнем шаге

применить классический алгоритм деления, то вся процедура потребует выполнения $2n$ элементарных операций умножения и $2n + 2$ операций сложения.

Если $p = 2^{nm-1} + c$, где $0 < c < b/2$. Тогда

$$b^n \equiv -2c \pmod{p}.$$

Значит для числа $A = A_1 + b^n A_2$, где $0 \le A_1, A_2 < b^n$,

$$A \equiv A_1 - 2cA_2 \pmod{p}.$$

Как видно, для вычисления редукции $2n$-значного числа по модулю такого n-значного числа Кронделла необходимо выполнить умножение n-значного числа на цифру, вычитание $(n + 1)$-значного из n-значного числа, и после этого вычислить редукцию $(n + 1)$-значного числа по n-значному модулю. Опять вся процедура потребует выполнения порядка $2n$ элементарных операций умножения и $2n + 2$ операций сложения.

Сравнение методов

Теоретические оценки вычислительной сложности рассмотренных методов однозначно отдают пальму первенства методам, базирующимся на числах специального вида. Однако интересно было бы сравнить их скорости на практике.

В ходе выполнения работы была написана библиотека функций, реализующих описанные методы. Также была написана библиотека функций, реализующих процессы формирования и проверки ЭЦП по ГОСТ Р 34.10-2001, позволяющая использовать специальные методы вычисления редукции в случае применения в качестве модуля кривой соответствующего числа. В качестве языка программирования был выбран C, легко переносимый между различными платформами.

Сравнение методов вычисления редукции

В ходе тестирования проводилось вычисление редукции 512-битного числа по 256-битному модулю. Так как методы вычисления редукции по числам Мерсенна и Кронделла зависят от выбора модуля, то было проведено три теста, в каждом из которых один из методов сравнивался с делением и универсальным методом Баррета по скорости вычисления (метод Монтгомери не рассматривался, т. к. его результат не есть остаток в чистом виде и требует дополнительной обработки, а его производительность сравнима с производительностью метода Барретта):

Тест №1 Модуль: $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ (обобщенное число Мерсенна P-256 из [5]). Специализированный метод: вычисление редукции по обобщённому числу Мерсенна.

Тест №2 Модуль: $p = 2^{255} + 1073$ (число Кронделла – тестовый модуль из ГОСТ Р 34.10-2001). Специализированный метод: вычисление редукции для числа Кронделла вида $p = 2^{nm-1} + c$.

Тест №3 Модуль: $p = 2^{256} - 3911$ (число Кронделла). Специализированный метод: вычисление редукции для числа Кронделла вида $p = b^n - c$.

Результаты измерения приведены в таблице 1. Для упрощения сравнения представлены не абсолютные значения времен выполнения, а отношения ко времени выполнения самого медленного метода – деления.

Таблица 1 Результаты измерений времени вычисления редукции различными методами

№ теста	Метод вычисления редукции	Время выполнения (в % к делению)
1	Деление	100.00

	Редукция Барретта	37.54
	Редукция Мерсенна	5.75
2	Деление	100.00
	Редукция Барретта	37.78
	Редукция Кронделла	17.77
3	Деление	100.00
	Редукция Барретта	37.45
	Редукция Кронделла	12.45

Видно, что применение специальных методов (там, где они применимы) позволяет получить ощутимый выигрыш в скорости вычисления модулярной редукции. Наибольший выигрыш даёт применение в качестве модуля обобщенного числа Мерсенна и соответствующего ему метода при вычислении редукции – почти в 17.5 (!) раз по отношению к тривиальному делению и в 6.5 раз по отношению к достаточно быстрому методу Барретта.

Однако возникает вопрос о том, насколько существенным будет этот выигрыш при вычислении всего процесса формирования/проверки цифровой подписи. На данный вопрос дают ответ результаты следующих тестов.

Сравнение производительности процессов формирования и проверки ЭЦП при использовании различных методов вычисления редукции

Проводились следующие тесты (в каждом тесте 1000 раз формировалась и проверялась цифровая подпись по алгоритмам ГОСТ Р 34.10-2001):

Тест №4 Исходные данные: кривая из контрольного примера ГОСТ Р 34.10-2001 (модуль $p = 2^{255} + 1073$ – число Кронделла). Используемые методы вычисления редукции: деление, редукция Барретта, редукция по модулю числа Кронделла вида $p = 2^{nm-1} + c$.

Тест №5 Исходные данные: кривая Р–256 из таблиц [5] (модуль – обобщенное число Мерсенна). Используемые методы вычисления редукции: деление, редукция Барретта, редукция по модулю обобщенного числа Мерсенна.

Результаты измерений представлены в таблице 2.

Теперь разрыв не столь значителен, однако же, по-прежнему существенен. Причем опять проигрывает не только вариант с использованием редукции обычным делением (который на практике почти не используется), но и широко применяемый метод вычисления редукции Барретта. По сравнению с ним использование специализированных модулей и алгоритмов позволяет ускорить процессы формирования/проверки подписи почти в 2 раза.

Таблица 2 Результаты измерений времени вычисления процессов формирования и проверки цифровой подписи по ГОСТ Р 34.10-2001 при использовании различных методов редукции

№ теста	Метод вычисления редукции	Время формирования подписи (в % к делению)	Время проверки подписи (в % к делению)
4	Деление	100.00	100.00
	Редукция Барретта	52.56	51.05
	Редукция Кронделла	37.09	35.52
5	Деление	100.00	100.00
	Редукция Барретта	52.53	51.16
	Редукция Мерсенна	26.50	25.05

Вывод

По результатам работы следует признать, что одной из мер по повышению производительности реализаций процессов ЭЦП, основанных на криптографии эллиптических кривых (и ГОСТ Р 34.10-2001 в частности), может служить применение в качестве модулей кривых чисел специального вида и соответствующих им методов редукции.
Представленное в работе исследование методов вычисления модулярной редукции позволяет при разработке таких реализаций выбирать наиболее эффективные с точки зрения производительности параметры схемы ЭЦП.

ЛИТЕРАТУРА:

1 Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А, Алгоритмические основы эллиптической криптографии – М.: 2000 г.

2 Домашев А.В., Грунтович М.М., Попов В.О., Правиков Д.И., Щербаков А.Ю. Программирование алгоритмов защиты информации – М.: «Нолидж», 2002.

3 A. Bosselaers, R. Govaerts, J. Vandewalle. Comparison of three modular reduction functions. Crypto '93, LNCS 773, 1994, pp. 175-186.

4 R.E. Crandall. Method and apparatus for public key exchange in a cryptographic system (Oct. 27, 1992), U.S. Patent #5,159,632.

5 NIST, Digital Signature Standard, FIPS Publication 186-2, February 2000

6 A. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. – CRC Press, 1996.

7 Peter L. Montgomery. Modular multiplication without trial division. Mathematics of Computation, v.44, n.170, 1985, pp. 519-521.

8 J. Solinas. Generalized Mersenne numbers. Technical Report CORR 99-39, Dept.of C&O, University of Waterloo, 1999.

Получено 12.10.2003. Доклад опубликован в Internet 18.10.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С. 37-44 . Секция- 3: Нормативное, методологическое и методическое обеспечение информационной безопасности
Пенза 2003 (http://beda.stup.ac.ru/04v/009)

ИНТЕРПОЛЯЦИОННЫЙ МЕТОД ВОССТАНОВЛЕНИЯ СИГНАЛА ПРИ ВОЗДЕЙСТВИИ ИМИТАЦИОННЫХ ПОМЕХ В РАДИОКАНАЛАХ С ЗАМИРАНИЯМИ

И. М. Орощук
Дальневосточный государственный технический университет

Разработки способов повышения устойчивости действующих телекоммуникационных радиосетей, чаще всего, основаны на принципах адаптации к дестабилизирующим факторам естественного и преднамеренного характера, имеющих приближенно одинаковую статистику. В данных условиях открывается возможность использования новых видов воздействия, основанных на применении имитационных помех (имитопомех), вызывающих нарушение режима обработки сигнала и самих сообщений за счет изменения параметров сигнала, в пределах установленных протоколом радиосети [1], что существенно затрудняет фиксировать факт преднамеренного воздействия. И так как статистики имитационных и естественных помех, как правило, существенно отличаются, используемые способы защиты от помех не обеспечивают устойчивую работу современных радиосетей [2]. При этом следует заметить, что с совершенствованием способов обработки сигналов расширяются возможности применения имитопомех, создавая в развитии технологий радиосвязи некоторое противоречие. Для решения данной проблемы необходимы исследования возможностей защиты систем радиосвязи от имитопомех в различных условиях их применения.

Настоящая статья посвящена вопросам защиты радиоканалов с замираниями от имитопомех, действующих во время сеанса связи. Замирания в радиоканалах вызваны проявлением интерференции большого числа лучей, отраженных от неоднородностей среды распространения [3]. Изменения состояния среды вызывают в точке приема случайные изменения амплитудных и фазовых характеристик сигнала. Введя в рассмотрение отношение уровней помехи и сигнала $h_{\text{п}} = U_{\text{п}}/U_{\text{с}}$ и его пороговое значение $h_{\text{п пор}}$, при котором обеспечивается эффективная имитоатака [4], можно рассмотреть три возможных ситуации. При $h_{\text{п}} < h_{\text{п пор}}^{-1}$ имеем существенное превышение уровня сигнала над помехой. В этом случае влиянием имитопомех можно пренебречь, так как классические методы обработки позволяют восстанавливать полезный сигнал. При $h_{\text{п}} > h_{\text{п пор}}$ обеспечивается устойчивый прием имитационных сигналов, при котором нападающая сторона может с максимальной скрытностью выполнять задачи имитоатаки. При этом для восстановления сигнала устойчиво работает метод исправления ошибок, основанный на выделении признаков различия символов имитопомехи и полезного сигнала [5], [6]. Наиболее сложной, с научной и практической точек зрения, является задача восстановления сигнала в случае примерного равенства интенсивностей имитопомехи и сигнала ($h_{\text{п пор}}^{-1} \le h_{\text{п}} \le h_{\text{п}}$). В этом случае сигнал в основном канале будет подвержен недопустимым краевым искажениям и дроблениям [4], что затрудняет восстановление пораженного

сигнала в основном канале, и, как следствие, восстановление методом исправления ошибок, используемым во втором случае [7]. В данной ситуации для восстановления сигнала можно применить оригинальный метод, основанный на интерполяции сигнала по данным анализа выделенных признаков различия символов имитопомехи и сигнала на интервале элементарной посылки, позволяющий в целом обеспечить комплексную защиту систем связи от имитопомех в различных состояниях канала. Рассмотрение этого метода и является предметом настоящей статьи.

Исходя из возможных состояний канала, для решения проблемы комплексной защиты канала при имитоатаке во время сеанса связи необходимо предусмотреть анализатор оценки $\hat{h}_{\text{п}}$, определяющий режим обработки сигнала (рис. 1, где представлена функциональная схема устройства комплексной защиты от имитопомех).

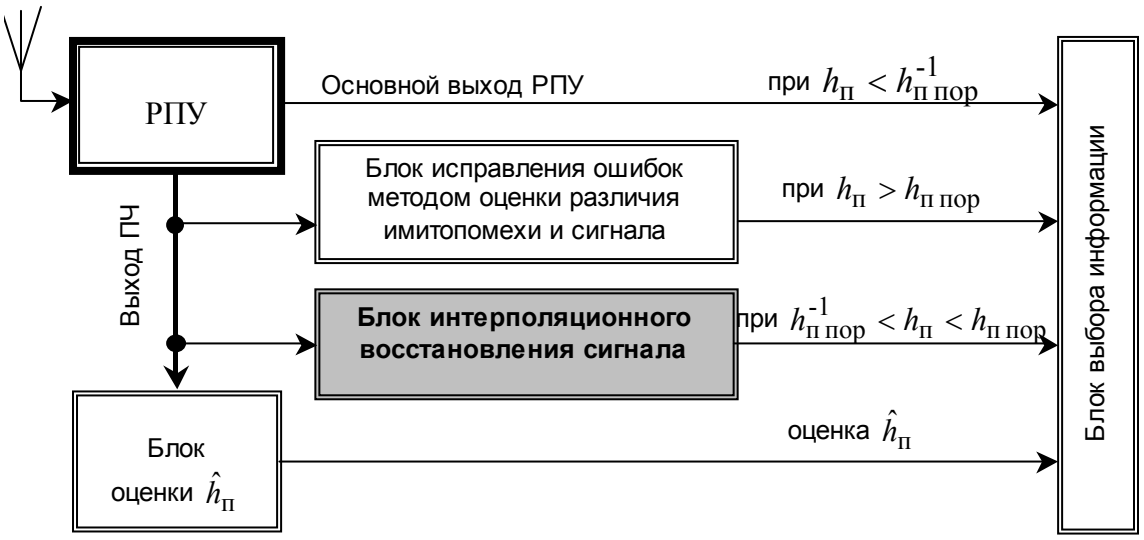


Рис. 1.

В данной схеме блок выбора информации по оценке $\hat{h}_{\text{п}}$ осуществляет выбор режима обработки сигнала: при $h_{\text{п}} < h_{\text{п пор}}^{-1}$ – используется основной канал приема, в случае, когда $h_{\text{п}} > h_{\text{п пор}}$ – метод исправления ошибок [7], а в моменты приближенного равенства уровней имитопомехи и сигнала предлагается использовать интерполяционный метод.

Интерполяционный метод основывается на использовании явления стохастических изменений времени задержки сигнала, регулярно наблюдаемых при распространении радиоволн в каналах с замираниями, в результате которых в силу некоррелированности трасс связи и имитоатаки в точке приема наблюдается случайный временной сдвиг фронтов первичных сигналов. В данном случае при приеме сигнала во время имитоатаки могут возникнуть три ситуации:

1. На всем интервале элементарной посылки наблюдается совпадение информационных символов имитопомехи и сигнала.
2. На интервале элементарной посылки наблюдается частичное совпадение информационных символов имитопомехи и сигнала (в первой или второй части посылки).
3. На всем интервале элементарной посылки наблюдается несовпадение информационных символов имитопомехи и сигнала.

Для восстановления сигнала в этих условиях, алгоритм интерполяционного метода строится на анализе признаков различия и совпадения информационных символов имитопомехи и полезного сигнала на протяжении каждой элементарной посылки, по которому в зависимости от возникающих ситуаций принимаются следующие решения:

- при 1-ой ситуации принятый символ дублируется;
- при 2-й ситуации решение принимается в пользу символа, соответствующего совпадающей части элементарной посылки;
- при 3-й ситуации формирование символа производится на основе анализа ближайшей ранее однозначно восстановленной элементарной посылки (по первому или второму варианту): в случае, если на последней части анализируемой посылки наблюдалось несовпадение символов – дублируется ранее однозначно восстановленный символ; если на последней части анализируемой посылки было совпадение символов – формируется символ противоположный ранее однозначно восстановленному (случай совпадения символов имитопомехи и полезного сигнала на протяжении всей посылки соответствует последнему варианту восстановления символа).

На рис. 2 иллюстрируется интерполяционный метод восстановления сигнала, на котором $U_{\text{С}}$ – первичный информационный сигнал; $U_{\text{И}}$ – последовательность импульсов имитопомехи; $U_{\text{С+И}}$ – сигнал на выходе основного канала приемника при воздействии имитопомех; $U_{\text{ИНТ}}$ – сигнал после восстановления; S_{i} – i-й символ сигнала; $\overline{S}_{\text{i}}$ – инверсия i-го символа).

С учетом того, что каналы связи используются при высоких отношениях сигнал-шум (более 10 дБ) при оценке эффективности исследуемого метода вероятностью возникновения ошибок в основном канале в случае совпадения символов полезного сигнала и имитопомехи можно пренебречь [4].

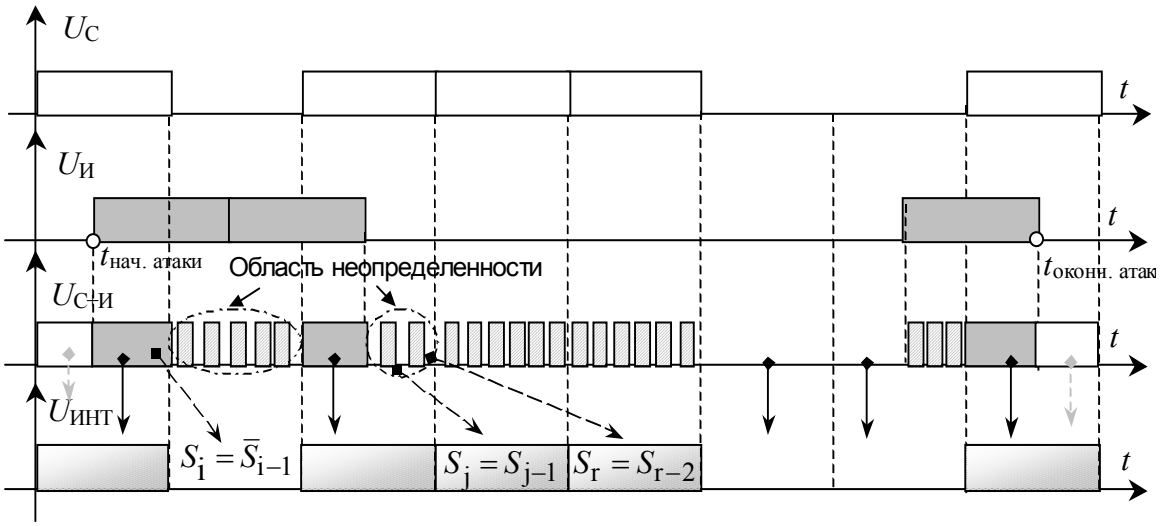


Рис. 2.

В данных условиях при использовании интерполяционного метода ошибка восстановления сигнала может возникнуть в случае, если время расхождения фронтов имитопомехи и сигнала не превысит разрешающую способность системы обнаружения их различия. Следовательно, для оценки эффективности метода необходимо провести статистический анализ расхождения фронтов имитопомехи и сигнала. Рассматривая декаметровые каналы связи, при распространении ионосферных радиоволн необходимо учесть влияние многолучевости [3], при котором каждый луч имеет случайное время задержки, в результате чего,

согласно центральной предельной теореме [8], время задержки фронта принимаемого суммарного сигнала для отдельной трассы будет с большой вероятностью стремиться к нормальному распределению:

$$w(t_з) = \frac{1}{\sigma_t \sqrt{2\pi}} \exp\left(- \frac{(t_з - \bar{t}_з)^2}{2\sigma_t^2} \right), \quad (1)$$

где $t_з$ – время задержки сигнала (фронта элементарной посылки); $\bar{t}_з$ – математическое ожидание времени задержки сигнала; σ_t – среднеквадратическое отклонение времени задержки фронта сигнала.

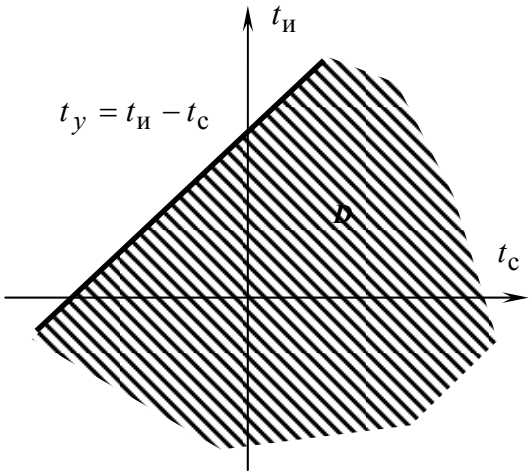


Рис. 3

Для оценки эффективности интерполяционного метода восстановления необходимо оценить величину разности времен задержки имитопомехи и сигнала: $t_y = t_и - t_с$. В данном случае плотность распределения времени задержки сигнала равна

$$w(t_с) = \frac{1}{\sigma_с \sqrt{2\pi}} \exp\left(- \frac{(t_с - \bar{t}_с)^2}{2\sigma_с^2} \right), \quad (2)$$

где $\sigma_с$ – среднеквадратическое отклонение времени задержки фронта сигнала; $\bar{t}_с$ – математическое ожидание времени задержки фронта сигнала.

Плотность распределения времени задержки фронта имитопомехи будет определяться выражением

$$w(t_и) = \frac{1}{\sigma_и \sqrt{2\pi}} \exp\left(- \frac{(t_и - \bar{t}_и)^2}{2\sigma_и^2} \right), \quad (3)$$

где $\sigma_и$ – среднеквадратическое отклонение времени задержки фронта имитопомехи; $\bar{t}_и$ – математическое ожидание времени задержки фронта имитопомехи. Определим совместную плотность распределения величины $t_y = t_и - t_с$. Для определения совместной плотности вероятности $w(t_y)$ необходимо вычислить интеграл по области *D*, находящейся ниже прямой $t_y = t_и - t_с$, как показано на рис. 3, т. е. при $t_y > t_и - t_с$:

$$P(t_и - t_с < t_y) = W(t_y) = \int_{-\infty}^{\infty} \int_{-\infty}^{t_y + t_с} w(t_с, t_и) dt_с dt_и. \quad (4)$$

С учетом большого пространственного разноса трасс случайные величины $t_и$ и $t_с$ будут независимы [9], в результате чего выражение (4) можно записать:

$$W(t_y) = \int_{-\infty}^{\infty} w(t_с) \left(\int_{-\infty}^{t_y + t_с} w(t_и) dt_и \right) dt_с ,$$

после дифференцирования которого по dt_y получим выражение для плотности распределения

$$w(t_y) = \int_{-\infty}^{\infty} w(t_c) w(t_y + t_c) dt_c \,. \qquad (5)$$

Далее, подставив в выражение (5) формулы (2) и (3), получим

$$w(t_y) = \frac{1}{2\pi\sigma_c\sigma_и} \int_{-\infty}^{\infty} \exp\left[-\frac{(t_c - \bar{t}_c)^2}{2\sigma_c^2} - \frac{(t_c - (\bar{t}_и - t_y))^2}{2\sigma_и^2} \right] dt_c \,. \qquad (6)$$

Опуская громоздкие вычисления формулы (6), запишем окончательное выражение для совместной плотности распределения:

$$w(t_y) = \frac{1}{\sqrt{2\pi(\sigma_c^2 + \sigma_и^2)}} \exp\left(-\frac{(t_y - (\bar{t}_и - \bar{t}_c))^2}{2(\sigma_c^2 + \sigma_и^2)} \right). \qquad (7)$$

Для дальнейших расчетов из выражения (7) получим плотность распределения относительной величины $\varepsilon_y = \frac{t_y}{\tau_0}$:

$$w(\varepsilon_y) = w(\varepsilon_y \tau_0) \frac{dt_y(\varepsilon_y)}{d\varepsilon_y} = \frac{\tau_0}{\sqrt{2\pi(\sigma_c^2 + \sigma_и^2)}} \exp\left(-\frac{(\tau_0\varepsilon_y - (\bar{t}_и - \bar{t}_c))^2}{2(\sigma_c^2 + \sigma_и^2)} \right), \qquad (8)$$

в результате преобразования выражения (8), получим

$$w(\varepsilon_y) = \frac{1}{\sqrt{2\pi(\tilde{\sigma}_c^2 + \tilde{\sigma}_и^2)}} \exp\left(-\frac{(\varepsilon_y - \Delta\bar{\varepsilon})^2}{2(\tilde{\sigma}_c^2 + \tilde{\sigma}_и^2)} \right), \qquad (9)$$

где ε_y – разностное время задержки, выраженное в долях элементарной посылки τ_0; $\Delta\bar{\varepsilon}$ – относительное значение разности математических ожиданий хода имитопомехи и сигнала; $\Delta\bar{\varepsilon} = (\bar{t}_и - \bar{t}_c)/\tau_0$; $\tilde{\sigma}$ – нормированное значение среднеквадратического отклонения временного сдвига фронта; $\tilde{\sigma} = \sigma/\tau_0$.

Известно, что система синхронизации реагирует только на временной сдвиг с точностью $\pm\tau_0/2$, без учета целой части, кратной τ_0. В данных условиях, если величина $\bar{t}_и - \bar{t}_c$ может принимать равным образом любые значения (так как, например, расстояние до объекта поражения из-за его движения и других обстоятельств точно неизвестно) – величина $\Delta\bar{\varepsilon}$ будет распределена по равномерному закону (в пределах $\Delta\bar{\varepsilon} = \pm 0{,}5$):

$$w(\Delta\bar{\varepsilon}) = 1 \,. \qquad (10)$$

В таком случае величина $\Delta\bar{\varepsilon}$ носит случайный характер с распределением (10), в результате чего выражение (9) будет уже определять условную плотность распределения $w(\varepsilon_y / \Delta\bar{\varepsilon})$. В случае, когда система имитоатаки ведет фазовую подстройку фронта имитопомехи, погрешность которой гораздо меньше предельных значений $\Delta\bar{\varepsilon}^* < \pm 0{,}5$, для дальнейшего расчета нужно пользоваться выражением (9).

Для первого случая, воспользовавшись Байесовским выражением полной вероятности, получим выражение для априорной функции распределения относительного сдвига фронтов имитопомехи и сигнала

$$w^*(\varepsilon_y) = \int_{-0{,}5}^{0{,}5} w(\Delta\bar{\varepsilon}) w(\varepsilon_y / \Delta\bar{\varepsilon}) d\Delta\bar{\varepsilon} = \frac{1}{\sqrt{2\pi(\tilde{\sigma}_c^2 + \tilde{\sigma}_и^2)}} \int_{-0{,}5}^{0{,}5} \exp\left(-\frac{(\Delta\bar{\varepsilon} - \varepsilon_y)^2}{2(\tilde{\sigma}_c^2 + \tilde{\sigma}_и^2)} \right) d\Delta\bar{\varepsilon} \,,$$

откуда получим:

$$w^*(\varepsilon_y) = \frac{1}{2}\left[\operatorname{erfc}\left(\frac{\varepsilon_y - 0{,}5}{\sqrt{2(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)}} \right) - \operatorname{erfc}\left(\frac{\varepsilon_y + 0{,}5}{\sqrt{2(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)}} \right) \right], \qquad (11)$$

где erfc(x) – дополнение интеграла вероятностей.

На основании полученной плотности распределения (11) определим оценку вероятности ошибки восстановления сигнала:

$$P_{\text{о.инт}} = \int_{-\frac{k}{2}}^{\frac{k}{2}} w^*(\varepsilon_y) d\varepsilon_y = \frac{1}{2} \int_{-\frac{k}{2}}^{\frac{k}{2}} \left[\operatorname{erfc}\left(\frac{\varepsilon_y - 0{,}5}{\sqrt{2(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)}} \right) - \operatorname{erfc}\left(\frac{\varepsilon_y + 0{,}5}{\sqrt{2(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)}} \right) \right] d\varepsilon_y, \qquad (12)$$

где k – относительная разрешающая способность системы обнаружения различия имитопомехи и сигнала; $k = \Delta t / \tau_0$ Δt – абсолютная разрешающая способность имитопомехи и сигнала. Вычисление интеграла (12) поэтапным методом подстановки дает следующий результат:

$$P_{\text{о.инт}} = k - \sqrt{\frac{2(\sigma_{\text{с}}^2 + \sigma_{\text{и}}^2)}{\pi}} \left(\exp\left(-\frac{(1-k)^2}{8(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)} \right) - \exp\left(-\frac{(1+k)^2}{8(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)} \right) \right) +$$
$$+ \frac{1-k}{2} \operatorname{erfc}\left(\frac{1-k}{\sqrt{8(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)}} \right) - \frac{1+k}{2} \operatorname{erfc}\left(\frac{1+k}{\sqrt{8(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)}} \right). \qquad (13)$$

Для практического применения упростим выражение (13). Полагая использование каналов при малых относительных среднеквадратических отклонениях фронта сигналов ($\widetilde{\sigma}_{\text{и(с)}} < 1$),

$$\int_{-\frac{k}{2}}^{\frac{k}{2}} \operatorname{erfc}\left(\frac{\varepsilon_y + 0{,}5}{\sqrt{8(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)}} \right) d\varepsilon_y \approx k \operatorname{erfc}\left(\frac{1}{\sqrt{8(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)}} \right),$$

исходя из чего выражение (12) с учетом накопления ошибки примет вид

$$P_{\text{о.инт}} \approx 2k \operatorname{erf}\left(\frac{1}{\sqrt{8(\widetilde{\sigma}_{\text{с}}^2 + \widetilde{\sigma}_{\text{и}}^2)}} \right) \qquad (14)$$

На рис. 4 показаны графики функции (14), из которых видно, что эффективность восстановления сигнала при малых относительных значениях среднеквадратического отклонения фронтов сигнала и имитопомехи ($\widetilde{\sigma}_{\text{с}}$ *и* $\widetilde{\sigma}_{\text{и}}$) определяется в основном разрешающей способностью системы обнаружения различия сигнала и имитопомехи – k. Снижение величины $P_{\text{о.инт}}$ происходит с ростом среднеквадратического отклонения фронта сигналов и при повышении скорости манипуляции.

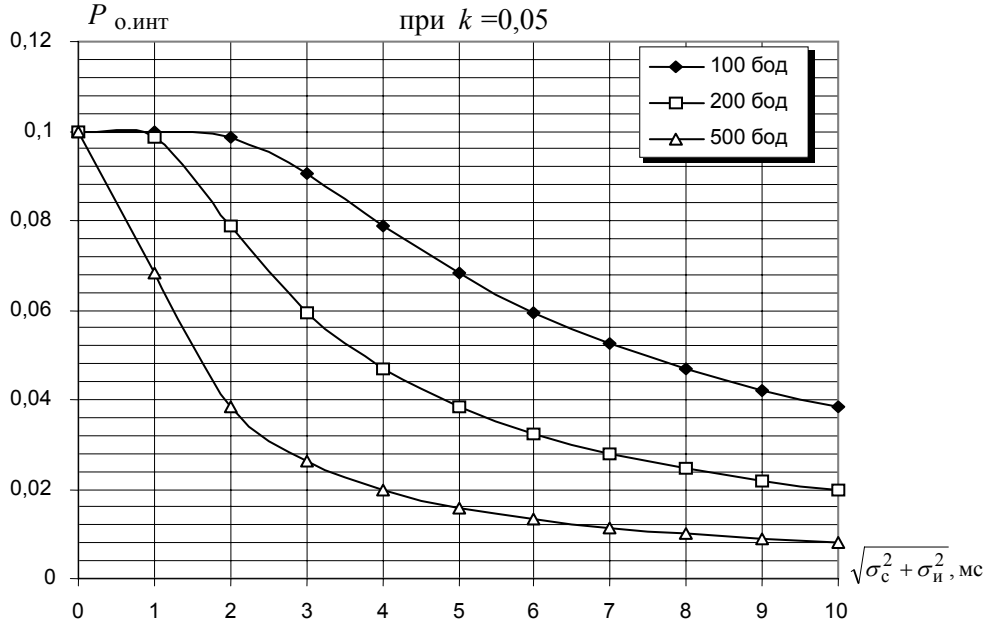


Рис. 4

Выводы:

Представленный метод позволяет в критических условиях (близких уровней сигнала и имитопомехи) восстанавливать полезный сигнал. При малых относительных среднеквадратических отклонениях фронтов сигналов эффективность восстановления в основном определяется разрешающей способностью системы обнаружения различия сигнала и имитопомехи (см. рис. 4). Повысить эффективность восстановления сигнала (при заданных параметрах радиотрассы) можно за счет искусственного повышения среднеквадратического отклонения фронтов сигнала $\sigma_{\text{с}}$ либо повышением скорости манипуляции в канале связи. Разработанный метод восстановления сигнала может быть использован для комплексной защиты каналов с регулярными замираниями при воздействии имитационных и других искусственных помех, создаваемых посторонними радиотехническими системами.

Литература:

1. Oroshchuk I.M. New technologies of unauthorized influence on automatic radio communication systems // The 3-rd international symposium «Sibconvers'99»: Proceedings. 18-20 May 1999. – Tomsk, TUSUR. – V.2. – pp. 336-338. (на английском).
2. Орощук И.М. Новые направления радиоэлектронного поражения автоматизированных систем радиосвязи // X Всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы». К 100-летию И.В. Курчатова: Сборник научных трудов. 28-30 января 2003 г. – М., МИФИ, 2003. – С. 138-140.
3. Долуханов М.П. Флуктуационные процессы при распространении радиоволн. М.: Связь, 1971. – 184 с.
4. Орощук И.М. Оценка имитостойкости канала с постоянными параметрами для фазоманипулированных сигналов при воздействии имитопомех // Радиотехника. – 2003. – № 1. – С. 22-28.

5. Oroshchuk I. The statistical detection method of unauthorized intrusions in the Rayleigh fading channel // 1st IEEE International Conference on Circuits and Systems for Communications: Proceedings. 26-28 June 2002. – St. Pb. State Polytechnic University Publishing House. – pp. 424-427. (на английском).
6. Орощук И.М. Метод обнаружения и фильтрации имитационных помех в рэлеевских каналах с замираниями // Безопасность информационных технологий. – 2002. – № 3. – С. 75-79.
7. Oroshchuk I.M. The filtering method of the digital radio channels by the frequency shift keying from the imitohindrances // 5th International Conference «Digital signal processing and its applications»: Proceedings-2. 12-14 March 2003. – Moscow, «Insvyazizdat». – 2003. – pp. 509-510. (на английском).
8. Левин Б.Р. Теоретические основы статистической радиотехники. М.: Радио и связь, 1989. – 656 с.
9. Стейн С., Джонс Дж. Принципы современной теории связи и их применение к передаче дискретных сообщений. / Перевод с англ. под ред. Л.М. Финка. М.: Связь, 1971. – 376 с.

Получено 15.10.2003. Доклад опубликован в Internet 22.10.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.45-48. Секция-4: Информационная безопасность телекоммуникаций
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/010)

Тезисы доклада

ОСОБЕННОСТИ ПОЛУЧЕНИЯ ДАННЫХ ПРОТОКОЛИРОВАНИЯ И АУДИТА В СРЕДЕ ОПЕРАЦИОННОЙ ПЛАТФОРМЫ IBM z/OS

Рыбалка А.А. E-mail: andrew@crystall.tl.ru
Научно – производственная фирма «Кристалл» (г. Пенза)

ОС IBM z/OS представляет собой сложную многокомпонентную и многофункциональную систему, содержащую несколько различных механизмов протоколирования и аудита событий и данных. Многие компоненты ОС, связанные с информационной безопасностью поддерживают протоколирование своих действий. Общий перечень таких компонентов, как правило установленных в системах на платформе z/OS, приведен таблице 1.

Таблица 1 – Перечень компонентов и функций z/OS, обеспечивающих протоколирование и аудит

Наименование	**Описание**
MVS	Центральная часть операционной системы, реализующая задачи системного уровня
RACF	Подсистема управления доступом к ресурсам
TSO/E	Терминальные приложения
DFSMS	Подсистема управления устройствами хранения данных
LDAP Server	Сервер LDAP. Элемент системного компонента Communication Server
Telnet Server	Сервер Telnet. Элемент системного компонента Communication Server
Web-server	Сервер WWW. Элемент системного компонента Communication Server
FTP server	Сервер FTP. Элемент системного компонента Communication Server
NFS server	Сервер NFS. Элемент системного компонента Communication Server
SNMP	Сервис SNMP. Элемент системного компонента Communication Server
SyslogD	Журнал регистрации Unix. Элемент системных компонентов USS & Communication Server
USS	Системные сервисы UNIX
SMF	Средство протоколирования событий
ORSS	Подсистема СУБД Oracle

Основным средством протоколирования и аудита в системе является System management facilities (SMF) - системное средство, позволяющее накапливать различную информацию, относящуюся к системе в целом и к отдельным задачам, включая и задачи информационной безопасности. Эта информация затем может анализироваться для составления отчетов, анализа событий и т. п. Помимо обеспечения поддержки информационной безопасности системы, данные SMF могут использоваться для учета работы пользователей, составления отчетов о надежности, анализа конфигурации, планирования заданий, профилировании использования системных ресурсов и наборов данных. Каждая

запись SMF представляет собой структуру данных, состоящую из стандартного заголовка, основной и (необязательно) дополнительных секций.

Основным объектом анализа состояния безопасности системы, безусловно, являются записи, регистрирующие события безопасности, фиксируемые подсистемой RACF. Существует три типа таких записей SMF80, 81, 83. Основным типом записи является тип 80 (RACF Processing). Каждая запись этого типа представляет собой сложную иерархическую структуру данных, подробно фиксирующую параметры выполняемой операции.

RACF формирует запись тип SMF80 в следующих случаях:

1) неавторизованные попытки входа в систему;

2) авторизованные попытки входа в систему;

3) авторизованный доступ или неавторизованные попытки доступа к ресурсам, защищенным RACF;

4) авторизованные или неавторизованные попытки модификации профилей в базе данных RACF.

В зависимости от установленных режимов, информация записей RACF SMF позволяет [10]:

– отслеживать общее использование критического ресурса (при установленном режиме ALL);

– идентифицировать ресурсы, относительно которых были неоднократно зафиксированы попытки неавторизованного доступа (при установленном режиме ALL или FAILURES);

– идентифицировать которые выполняли зафиксированные неавторизованные запросы;

– отслеживать активность пользователей, имеющих атрибут SPECIAL;

– отслеживать активность отдельных пользователей.

Кроме собственно событий безопасности, в публикации [11] настоятельно рекомендуется ни в коем случае не отключать регистрацию следующих IBM SMF записей: SMF00 (IPL, инициализация системы), SMF07 (Потерянные Данные SMF), SMF30 (Общая Работа Адресного пространства), SMF70-SMF79 (Средство Управления ресурсами или RMF), и SMF90 (Системная Среда). Эти записи имеют отношение непосредственно с критическими частями среды MVS и не имеют никаких избыточных копий.

Помимо этого, MVS поддерживает системный журнал регистрации SYSLOG, в котором фиксируются различные сообщения о системных событиях. SYSLOG, фактически, представляет собой системную информационную консоль, сообщения которой периодически выгружается в заданный набор данных. Так, например, RACF дублирует в системный журнал оповещения владельцам ресурсов о попытках неавторизованного доступа к их ресурсам [9]. Записи выводятся в последовательный набор данных (sequential data set, SDS). Этот набор данных представляет собой текстовый файл, в котором каждая запись представляет собой переменный блок (VB) данных, состоящий из заголовка установленного формата и самого сообщения в свободной форме.

Как правило, записи системного журнала носят обобщенный характер и оперативно информируют оператора об общем состоянии компонента или функции системы. Поскольку в заголовке записи не содержится информации, однозначно определяющей этот компонент или функцию (в качестве источника сообщения указывается идентификатор задания/терминала/задачи), точно идентифицируются они путем визуального лексического разбора самого

сообщения. Несколько сообщений, идущие подряд от одного источника, могут перебиваться сообщениями от других источников, что, потенциально, затрудняет их анализ, при отсутствии вспомогательных средств.

Среди записей системного журнала есть и такие, которые непосредственно характеризуют состояние информационной безопасности системы. Например, это записи об активации/деактивации подсистемы контроля доступа RACF или сообщения об успешном/неуспешном доступе к терминальным приложениям.

Журнал регистрации Unix, поддерживаемый сервисом SyslogD, используется, главным образом элементами z/OS Unix System Services (USS) и Communication Server (CS). В значительной степени, информация этого журнала регистрации связана с использованием стека TCP/IP. Поскольку подсистема Oracle, на которой построена большая часть прикладных систем в среде z/OS, доступна именно через стек TCP/IP, данный журнал может содержать значимую информацию для проведения анализа информационной безопасности.

Сервис SyslogD представляет собой стандартный сервис UNIX Syslog, портированый в среду z/OS USS. SyslogD позволяет сортировать сообщения по источникам и по степени важности. Система дает возможность осуществлять запись сообщений в различные файлы регистрации, выводить на консоль или отправлять по сети на удаленный хост, используя сервис протокола TCP/IP. На основе SyslogD возможна организация централизованной регистрации для сети.

Кроме этого, некоторые подсистемы (JES, RACF) и приложения (TSO) ведут собственное протоколирование связанных с ними событий [9]. RACF обеспечивает сбор статистики доступа (количества обращений) к защищенным ресурсам, которая накапливается в базе RACF. Поскольку доступ к результатам такого протоколирования возможен, главным образом, средствами самих приложений-источников протоколирования, их использование для проведения автоматизированного анализа внешними средствами затруднительно.

В принципе, наборы данных SMF, являющиеся центральным хранилищем данных протоколирования и аудита, включают и информацию, которая обеспечивается другими механизмами протоколирования, однако в ряде случаев (например, для анализа этапа начальной загрузки системы (IPL)), может оказаться более удобным обращение к системным журналам регистрации.

Основные сравнительные характеристики различных механизмов протоколирования и аудита, важные с точки зрения выбора того или иного механизма, приведены в таблице 2.

Таблица 2 – Характеристики механизмов протоколирования и аудита

Характеристика	**MVS SMF**	**MVS SYSLOG**	**z/OS USS SyslogD**
Формат записей	FVB («fixed» variable block)	VB (variable block)	VB
Стандартный заголовок (время/дата/тип:источник)	есть	есть	есть
Описание событий	Подробное дискретное описание каждого события	Сообщение свободной формы	Сообщение свободной формы
Область фиксируемых событий	Система в целом и отдельные задания	Система в целом и отдельные задания	События, связанные с компонентами USS и CS

Характеристика	MVS SMF	MVS SYSLOG	z/OS USS SyslogD
Автоматизированный анализ записей	Удобен	Затруднен, необходим лексический разбор каждого сообщения	Затруднен, необходим лексический разбор каждого сообщения
Визуальный анализ записей	Затруднен, бинарный набор данных	Удобен, текстовый набор данных	Удобен, текстовый набор данных
Необходимость дополнительных средств для анализа	Требуется программа генерации отчетов	Дополнительные средства необязательны	Дополнительные средства необязательны
Удаленный доступ к данным	Через разделяемую файловую систему	Через разделяемую файловую систему	Возможна пересылка сообщений на удаленный сервер Syslog
Влияние на систему	Высокое, при некорректной работе возможен крах	Невысокое	Невысокое
Пригодность данных для различных видов анализа			
Сигнатурный анализ	Возможен	Возможен	Возможен
Статистический анализ	Возможен	Затруднен	Затруднен
Анализ потребления ресурсов	Возможен	Невозможен	Невозможен

Из таблицы видно, что для автоматизированного анализа оптимальными являются данные SMF, как с точки зрения формата хранения, так и с точки зрения полноты информации о событиях. Вместе с тем, использование данных SMF предполагает значительные затраты ресурсов для выполнения тонкой настройки системы и разработки/приобретения средств автоматизированного анализа данных.

Литература:

9. С. Симонов, П. Колдышев. Обеспечение информационной безопасности в вычислительных комплексах на базе манфреймов. М: Информационный бюллетень JetInfo № 4 (107)/2002.

10. SA22-7682-03 z/OS V1R4.0 Security Server RACF Macros and Interfaces, Fourth Edition, September 2002.

11. Mark S. Hahn. Data Security and SMF. ©1995 CANDLE Corporation. (http://www.geocities.com/SiliconValley/Peaks/4170/articles/smfdata1.htm)

Получено 20.10.2003. Доклад опубликован в Internet 24.10.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.49-52. Секция-7: Аудит информационной безопасности
Пенза-декабрь-2003 (http://beda.stup.ac.ru/RV-conf/v04/011)

СПОСОБ ОПРЕДЕЛЕНИЯ ПРИНАДЛЕЖНОСТИ ТОЧКИ МНОГОМЕРНОЙ ВЫБОРКЕ

Лакин К.А., Сапегин Л.Н. *НПФ "Кристалл"*

Введение

Теория принятия решений в последние годы приобрела большое значение в области информационной безопасности. В данной статье рассматривается задача определения принадлежности точки многомерной выборке как части задачи принятия решения.

В результате процесса кластеризации из совокупности многомерных статистических данных выделяется одна или несколько выборок (кластеров) достаточно большого объема. Кластеры малых объемов игнорируются. Пусть одна из выделенных выборок (ее объем обозначается через N) представляется точками $X_i = (x_1^i, x_2^i, ..., x_n^i)$, $i = 1\text{-}N$ в n-мерном числовом пространстве. Для заданной точки $X = (x_1, x_2, ..., x_n)$ требуется принять решение о принадлежности точки X к выборке с заданной вероятностью ε ошибки первого рода. Другими словами, если X генерирована по закону выборки, то она ошибочно может быть не причислена к этой выборке с вероятностью не более ε.

Решение задачи видится в форме замкнутой огибающей поверхности размерности n–1, содержащей внутри $(1-\varepsilon)N$ точек выборки и εN точек вне. Тогда при попадании точки X внутрь поверхности принимается решение о принадлежности точки X к выборке. При $n = 2$ такой «поверхностью» может быть контур прямоугольника или эллипс, при $n = 3$ – поверхность параллелепипеда или эллипсоида. Проблемы, возникающие при нахождении огибающей поверхности в n-мерном пространстве, можно представить на примерах в плоскости ($n = 2$) и в пространстве ($n = 3$).

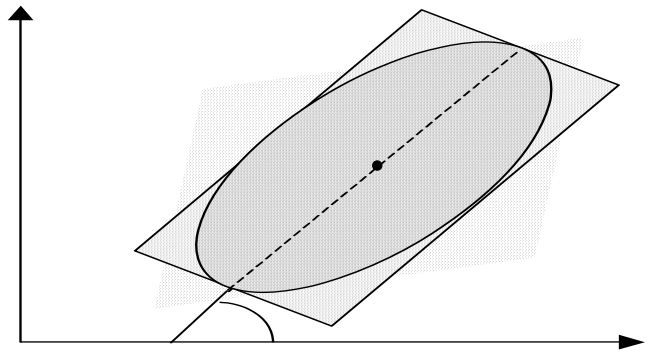


Рисунок 1 – Огибающие «поверхности» прямоугольника и эллипса

Кажется, что проще всего по данной совокупности точек найти прямоугольник (n-мерный параллелепипед), содержащий примерно $(1\text{-}\varepsilon)N$ точек. Однако, в случае зависимых координат он повернут относительно осей координат (см. рисунок 1), и следовательно, потребуется найти центр и косинусы углов

поворота множества точек, чтобы преобразовать огибающую поверхность к каноническому виду: $u_j \le x_j \le v_j$; $j = 1 \div n$, а затем подобрать размеры (u_j, v_j) так, чтобы n-мерный параллелепипед содержал, по крайней мере, $(1-\varepsilon)N$ точек. Тогда критерий принадлежности точки X выборке состоит в следующем: координаты данной точки $X = (x_1, x_2, ..., x_n)$ сначала пересчитываются по каноническому преобразованию, а затем покоординатно сравниваются с пороговыми значениями (u_j, v_j), $j = 1\text{-}n$. Точка X принимается выборкой, если пересчитанные координаты $(x_1^{'}, x_2^{'}, ..., x_n^{'})$ удовлетворяют неравенствам: $u_j \le x_j^{'} \le v_j$; $j = 1 \div n$, иначе X отвергается.

Более точной (с меньшей вероятностью ошибки второго рода) огибающей поверхностью является n-мерный эллипсоид, однако для получения его уравнения снова потребуется найти центр и косинусы углов поворота, а также подобрать длины его осей. Точка X принимается выборкой, если при подстановке ее координат в уравнение эллипсоида получается значение меньше 0, иначе X отвергается.

Обе описанные выше проблемы в принципе теоретически разрешимы, но практические трудности очень велики уже при $n \approx 10$. Кроме того, на практике ядро (основная масса) совокупности точек многомерной выборки может иметь более сложную форму, чем параллелепипед или эллипсоид. В этих случаях точная граница ядра аналитически не может описываться поверхностями первой или второй степени. А нужно ли знать уравнение границы ядра, чтобы определить: внутри или вне находится данная точка X?

Принадлежность точки многомерной выборке

Рассмотрим точку δX на луче $[0, X)$ и вне ядра, взяв постоянную δ достаточно большой. Найдем все расстояния $d_i = \sqrt{\sum_{j=1}^{n} (\delta x_j - x_j^i)^2}$; $i = 1 \div N$, от точки δX до точек X_i и выберем s наименьших d_i (пусть это будут: $d_1, d_2, \ldots, d_s$). Тогда точки $X_1, X_2, \ldots, X_s$ находятся где-то на границе или у границы ядра. Сравнивая расстояние точки X до центра 0 с расстояниями до центра точек $X_1, X_2, \ldots, X_s$, можно определить, где находится точка X по отношению к граничным точкам: ближе к центру 0 или дальше, т.е. внутри или вне ядра.

Эта идея берется за основу в следующем алгоритме определения принадлежности точки многомерной выборке.

Предлагаемый алгоритм состоит из следующих этапов:

1) выделение ядра выборки;

2) нахождение точки X_0 – центра ядра, радиуса R и расстояния r точки X до центра X_0;

3) нахождение точек $X_{i1}, X_{i2}, \ldots, X_{is}$ у границы, ближайших к точке $R \cdot r^{-1} X$.

4) вычисление расстояний точек $X_{i1}, X_{i2}, \ldots, X_{is}$ до центра и принятие решения.

Этап 1. Выделение ядра выборки состоит из центрирования и нормирования выборки с последующим удалением «аномальных» точек. Центрирование и нормирование делается по формуле:

$$x_j^i := (x_j^i - \overline{x_j}) s_j^{-1}, \qquad \textbf{(1)}$$

где $\overline{x_j} = \frac{1}{N}\sum_{i=1}^{N} x_j^i$;

$$s_j = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_j^i - \overline{x_j})^2}\ ;$$

i = 1-N;

j = 1-n.

Центрированная и нормированная выборка обозначается теми же буквами:

$$X_i = (x_1^i, x_2^i, ..., x_n^i),\ i = 1\text{-}N.$$

Точка X_i удаляется из выборки (или корректируется и оставляется), если хотя бы одна координата по модулю превосходит некоторое значение $c > 1$ (если $c = 3$, то удаляются точки, имеющие координаты со значениями вне 3σ-интервала, $\sigma = 1$). Оставшиеся точки снова центрируются и нормируются, чтобы учесть отсутствие «аномальных» точек. Полученная таким образом выборка называется ядром исходной выборки. Число точек в ядре выборки будем также обозначать через N. Отношение числа «аномальных» точек к числу всех точек первоначальной выборки является оценкой ε. Уменьшить значение ε, если это требуется, можно увеличением значения параметра c.

Этап 2. Центр ядра (точка X_0) находится как $X_0 = (\overline{x_1}, \overline{x_2}, ..., \overline{x_n})$, где $\overline{x_j} = \frac{1}{N}\sum_{i=1}^{N} x_j^i$, j = 1-n. Все значения $\overline{x_j}$ должны быть практически равными нулю. Для контроля вычислений вывести $\max\limits_{1 \le j \le n} |\overline{x_j}|$ на печать и положить $X_0 := (0, 0, \ldots, 0)$. Радиус R и расстояние r от точки X до центра X_0 определяются по формулам (2) и (3), соответственно.

$$r = \sqrt{\sum_{j=1}^{n}(x_j)^2}\ ; \qquad \textbf{(2)}$$

$$R = \max_{1 \le i \le N} \sqrt{\sum_{j=1}^{n}(x_j^i)^2}\ . \qquad \textbf{(3)}$$

Этап 3. Вычислить расстояния d_i, i = 1-N от точки $R \cdot r^{-1} \cdot X$, находящейся вне ядра, до точек X_i, i = 1-N, ядра по формуле (4).

$$d_i = \sqrt{\sum_{j=1}^{n}(R \cdot r^{-1} \cdot x_j - x_j^i)^2}\ . \qquad \textbf{(4)}$$

Индекс i в формуле (4) изменяется в пределах от 1 до N включительно.

Найти s наименьших значений $d_{i1} \le d_{i2} \le \ldots \le d_{is}$, где $s = 1, 3, 5, \ldots$ – третий параметр алгоритма наряду с ε и c. Соответствующие точки границы ядра: $X_{i1}, X_{i2}, \ldots, X_{is}$ (см. рисунок 2 при $s = 3$).

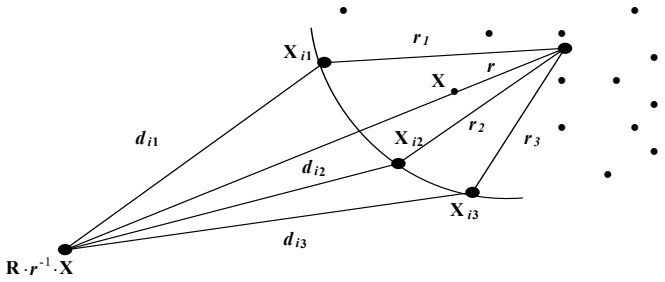


Рисунок 2 – Расположение *X* относительно границы

Этап 4. Вычислить расстояния $r_1, r_2, \ldots, r_s$ точек $X_{i1}, X_{i2}, \ldots, X_{is}$ до центра $X_0 := (0, 0, \ldots, 0)$ (см. рисунок 2) по формуле (5).

$$r_k = \sqrt{\sum_{j=1}^{n} (x_j^{ik})^2}. \qquad \textbf{(5)}$$

Индекс k в формуле (5) изменяется в пределах от 1 до s включительно.
Составить разности: $(r_1–r)$, $(r_2–r)$, …, $(r_s–r)$. Принять решение:

- если большинство разностей положительно, то точка X внутри ядра; следовательно, X принадлежит выборке;
- если большинство разностей отрицательно, то точка X вне ядра; при этом:
- если большинство модулей разностей не превосходит d, то считается, что X принадлежит выборке (но может не принадлежать ядру);
- если большинство модулей разностей превосходит d, то X не принадлежит ни ядру, ни выборке.

Здесь d – четвертый устанавливаемый параметр алгоритма наряду с параметрами ε, c, s. Можно рекомендовать значение d, равное среднему расстоянию между точками ядра выборки.

Вывод

Предложенный способ определения принадлежности точки многомерной выборке может найти применение в задачах разбора данных аудита, распознавания образов и многих других областях применения теории принятия решения. Данный способ позволяет учесть погрешности принадлежности точки многомерной выборке, оценить «истинную» форму кластеров и включить эти данные в процедуру принятия решений.

Таким образом, предложенный метод представляет интерес для различных областей знаний и практических приложений.

Получено 25.10.2003. Доклад опубликован в Internet 26.10.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.53 -55. Секция-7: Аудит информационной безопасности
Пенза-декабрь-2003 (http://beda.stup.ac.ru/RV-conf/v04/012)

СИНТЕЗ ПРАВИЛА ДЛЯ АНАЛИЗА ПРОТОКОЛА ДИФФИ-ХЕЛМАНА

Давыдов А.Н. НПФ «Кристалл»

Нотация BAN-логики

В BAN логике [1] выделяют следующие объекты: пользователи, ключи, и формулы (также называемые утверждениями). Символы A и B обозначают пользователей; символы X и Y обозначают дополнительные утверждения; символ K обозначает ключи шифрования.

Единственная пропозициональная связка является конъюнкцией, и обозначается запятой. Конъюнкция рассматривается как множество, обладающее свойствами ассоциативности и коммутативности. Помимо конъюнкции используются следующие конструкции:

$A \models X$: A верит утверждению X; в частности, A должен действовать так, как будто X верно.

$A \triangleleft X$: A видит утверждение X. Некто послал сообщение, содержащее утверждение X пользователю A; пользователь A может прочитать и повторить утверждение X (возможно после выполнения расшифрования).

$A \mid\sim X$: A однажды сказал утверждение X; пользователь A когда-то послал сообщение, включающее утверждение X; не известно когда было послано сообщение: давно или в течение работы протокола, но известно, что пользователь A верил утверждению X, когда его отправлял.

$A \Rightarrow X$: A имеет право на X и должен быть доверенным для этого. Эта формула используется, когда участник делегирует право на некоторое утверждение X другому участнику. Например, ключи шифрования в некоторых протоколах доверяются генерировать определенным серверам. Это можно выразить формулой, интерпретируемой как предположение, что участники доверяют серверу генерацию ключей для них с требуемым качеством.

#(X): утверждение X является свежим; под термином «свежий» понимается, что утверждение X не было послано до начала работы протокола; данная конструкция полезна для нонсов - выражений специально генерируемых для того, чтобы, доказать, что сообщение является свежим; нонсы обычно включают отметку времени или число, которое используется только один раз, например, порядковый номер сообщения.

$A \overset{K}{\longleftrightarrow} B$: пользователи A и B могут использовать общий ключ K, для установки связи; ключ K известен только пользователям A и B, или другим пользователям, которым A или B доверяют; другим пользователям ключ K не известен.

$A \overset{X}{\Leftrightarrow} B$: утверждение X является секретом известным только пользователям A и B, и, возможно, пользователям, которым они доверяют; только A и B могут использовать X, для доказательства подлинности заявленных идентификаторов друг другу. Часто X является также и свежим. Пример общего секрета – пароль.

$\{X\}_K$: шифротекст от X на ключе K. Подразумевается, что есть указатель, что это сообщение от A, а также, что A в состоянии узнать свое сообщение и игнорировать его у себя на приеме.

$\langle X \rangle_Y$: объединение (конкатенация) утверждения X и секрета Y; присутствие Y доказывает подлинность идентификатора того, кто передал $\langle X \rangle_Y$. На практике это может быть просто X||Y, где Y – пароль. Y играет роль доказательства источника X. Это обозначение напоминает $\{X\}_K$, где также содержится доказательство подлинности идентификатора источника сообщения через знание секрета К.

Описание протокола Диффи-Хелмана

Целью протокола ключевого обмена Диффи-Хелмана [2] является формирование пользователями A и B отрезка битов, известного только им, путем использования передач по открытому каналу связи. Протокол неявного ключевого обмена Диффи-Хелмана представлен на рисунке 3.

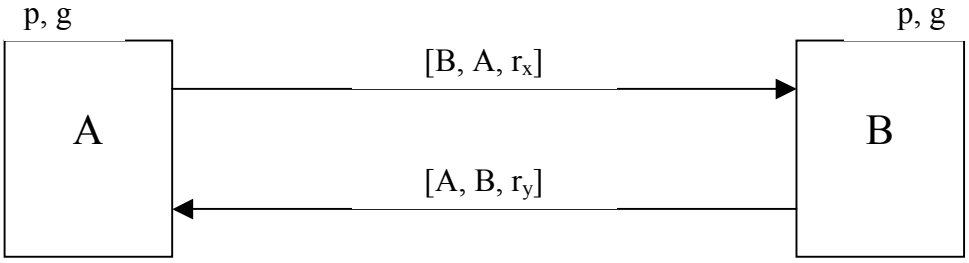


Рисунок 3 – Протокол Диффи-Хелмана

На шаге 1 пользователь A генерирует случайное n–разрядное число x от своего ДСЧ, вычисляет число $r_x = g^x (\mathrm{mod}\ p)$ и передает его B в форме сообщения [B, A, r_x]. На шаге 2 пользователь B генерирует случайное n–разрядное число y от своего ДСЧ, вычисляет число $K_{ab} = r_x^y (\mathrm{mod}\ p)$ и считает его секретным ключом для связи с A; вычисляет число $r_y = g^y (\mathrm{mod}\ p)$и передает его A в форме сообщения [A, B, r_y]. На шаге 3 пользователь A вычисляет число $K_{ba} = r_y^x (\mathrm{mod}\ p)$ и считает его секретным ключом для связи с B. Поскольку $r_x^y = r_y^x$, то $K_{ab} = K_{ba}$.

Предполагается, что все вычисления в протоколе выполняются в арифметике по модулю p с примитивным элементом g в качестве основания степени. Все числа, включая p и g, имеют достаточно большую разрядность n для обеспечения безопасности протокола.

Синтез правила для анализа протокола Диффи-Хелмана

Для записи правила анализа протокола Диффи-Хелмана в знаменатель нужно записать конечную цель протокола, а именно $A \xleftrightarrow{K} B$, что означает, что пользователи A и B могут использовать общий ключ K, для установления связи; ключ K известен только пользователям A и B, и не известен другим пользователям. В числитель правила следует записать утверждения доверия, которые необходимо допустить до выполнения протокола (предположения), и получить при выполнении протокола. Для протокола Диффи-Хелмана нужно сделать следующие предположения:

– субъекты A и B доверяют системе, в которой они функционируют, то есть они доверяют открытым параметрам системы p и g: $A \models p$, $A \models g$, $B \models p$, $B \models g$. То что субъекты A и B доверяют параметрам системы p и g подразумевает под собой следующее:

- числа p и g имеют достаточно большую разрядность для обеспечения безопасности протокола;

- злоумышленник не может модифицировать значения чисел p и g;
- субъекты A и B всегда могут получить у системы значения чисел p и g.

– субъект A доверяет, что субъект B генерирует хорошее случайное число y, имеющее достаточно большую разрядность: $A \models B \Rightarrow y$;

– субъект B доверяет, что субъект A генерирует хорошее случайное число x, имеющее достаточно большую разрядность: $B \models A \Rightarrow x$;

– субъект A верит, что он генерирует свежее число x; под термином «свежий» подразумевается, что A не генерировал такое же значение числа x ранее;

– субъект B верит, что он генерирует свежее число y.

Следующие утверждения возникают в ходе выполнения протокола:

– субъект A заявил утверждение r_x: $A \mid\sim r_x$;

– субъект B заявил утверждение r_y: $B \mid\sim r_y$;

– субъект A получил утверждение r_y: $A \triangleleft r_y$;

– субъект B получил утверждение r_x: $B \triangleleft r_x$.

Следующие утверждения должны выводиться из анализа протокола взаимной аутентификации, который предшествует протоколу Диффи-Хелмана или интегрирован в него:

– субъект A верит, что утверждение r_y прислал субъект B: $A \models B \mid\sim r_y$;

– субъект B верит, что утверждение r_x прислал субъект A: $B \models A \mid\sim r_x$;

– субъект A верит, что утверждение r_y свежее: $A \models (\#r_y)$;

– субъект B верит, что утверждение r_x свежее: $B \models (\#r_x)$.

Если два первых утверждения не верны, то возможна атака на протокол «человек по середине». Если два первых сообщения не верны, то возможна атака повтора.

Таким образом, правило анализа протокола Диффи-Хелмана записывается в нотации BAN логики в виде формулы (6).

$$\frac{A \mid\equiv p, A \mid\equiv g, B \mid\equiv p, B \mid\equiv g, A \mid\equiv B \Rightarrow y, B \mid\equiv A \Rightarrow x, A \mid\equiv (\#x), B \mid\equiv (\#y),}{A \overset{K}{\longleftrightarrow} B}$$

$$\frac{A \mid\sim r_x, B \mid\sim r_y, A \triangleleft r_y, B \triangleleft r_x, A \mid\equiv B \mid\sim r_y, B \mid\equiv A \mid\sim r_x, A \mid\equiv (\#r_y), B \mid\equiv (\#r_x)}{A \overset{K}{\longleftrightarrow} B} \qquad (6)$$

Литература

1. Michael Burrows, Martin Abadi, Roger Needham. A Logic of Authentication. – ACM Translations in Computer Systems, 8(1): 18-36, February 1990.

2. Alfred Menezes, Paul van Oorschot, Scott Vanstone. Handbook of applied cryptography. – CRC Press, October 1996.

Получено 25.10.2003. Доклад опубликован в Internet 26.10.2003.

Труды научно-технической конференции

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.56-59. Секция-4: Анализ вычислительной среды, верификация, сертификация программ.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/013)

КОНТРОЛЬ СООТВЕТСТВИЯ ЭЛЕКТРИЧЕСКИХ СХЕМ, ВЫПОЛНЯЕМЫХ НА ПЛИС, ИХ ИСХОДНОМУ ОПИСАНИЮ

Кулагин О.В., Чижухин Г.Н.
Пензенский научно-исследовательский электротехнический институт,
Пензенский государственный университет

Введение. Для контроля соответствия разрабатываемой электрической схемы ее исходному описанию обычно используется моделирование на предварительно определенных тестовых наборах. Оно позволяет не только проанализировать схему на риски сбоя, но и оценить в целом ее работоспособность по виду выходных сигналов схемы, формируемых в процессе моделирования. Однако, очень сложно составить тестовые наборы, полностью определяющие работоспособность больших схем, а моделирование их весьма громоздко. Поэтому, необходим способ контроля без моделирования соответствия описания полученной схемы (далее – *полученного описания*) исходному описанию, причем контроль соответствия схем, выполненных в виде отдельных печатных плат (далее – *проверка плат*), будет несколько отличаться от контроля схем на ПЛИСах (далее – *проверки ПЛИС*).

Особенности проверки плат. Рассмотрим процесс проектирования плат на примере САПР P-CAD 4.5. Он включает следующие этапы:

1. Ввод принципиальной схемы (файл с расширением SCH) с использованием библиотеки элементов (каждый элемент – файл с расширением SYM).
2. Преобразование схемы в печатную плату (файл с расширением PCB), включая ввод чертежа платы, размещение элементов на плате и разводку платы. При этом каждому элементу принципиальной схемы (файлу с расширением SCH) необходимо поставить в соответствие чертеж его корпуса (файл с расширением PKG).

Для файлов принципиальных схем (расширение SCH) и файлов печатных плат (расширение PCB) предусмотрена возможность формирования текстового описания соединений схемы в формате CMP. Файл CMP представляет собой последовательность записей, каждая из которых соответствует одному элементу схемы (т.е. файлу с расширением SYM или PCB), и включает: 1) имя файла элемента; 2) конструктивное обозначение элемента; 3) список цепей, приходящих на контакты элемента в виде пар «контакт – цепь». Так как в этой записи указываются все контакты элемента, то для неподключенных контактов вместо имени цепи указывается пустая строка.

Использование единого формата CMP для описания соединений в принципиальной схеме и на плате, а также для определения однозначного соответствия между ними позволяет получать одинаковые описания исходной и полученной схемы, которые можно сравнивать между собой.

Особенности проверки ПЛИС. Рассмотрим процесс проектирования схем на ПЛИСах фирмы Xilinx при помощи САПР Foundation Series. Если в предыдущем случае исходная схема и полученное описание имеют общий формат и будут полностью совпадать в случае правильной разводки платы, то этого нельзя сказать про схему, выполняемую на ПЛИС.

Форматы исходной схемы и полученного описания в данной САПР ПЛИС разные – для исходных схем используется формат XNF, а для готовых – формат EDIF (файл с расширением EDN). Кроме того, в описание исходной схемы вносятся следующие изменения в процессе ее перенесения на ПЛИС: 1) показывается цепь начального сброса/установки триггеров GSR по включению питания, невидимая на этапе ввода исходной схемы; 2) проходные буферы выходных сигналов показываются как формирователи третьего состояния с неактивным входом перевода в это состояние; 3) комбинаторные узлы приводятся в базис И – ИЛИ – НЕ – Исключающее ИЛИ (с выделением инверсий по входам и выходам логических элементов в отдельные инверторы); 4) логические элементы с большим числом входов разбиваются на группу однотипных элементов, каждый из которых имеет не более пяти входов; 5) во всех триггерах показываются входы S, R, CE, C, D вне зависимости от реально используемых входов.

Поэтому для сравнения исходного и полученного описаний схемы на ПЛИС необходимо выполнить ряд равносильных преобразований полученного описания с тем, чтобы: 1) удалить из исходного и полученного описания неиспользуемые контакты элементов, например подключенные к земле входы дизъюнкторов, и т.п.; 2) унифицировать комбинаторные узлы исходного и полученного описаний; 3) сравнить описания схем. Кроме того, исходное и полученное описания схемы необходимо для выполнения равносильных преобразований перевести в алгебраическую форму, в частности, представить их в виде тензорных уравнений (ТУ), для формирования которых используется тензорная алгебраическая система (ТАС) [1].

Удаление неиспользуемых контактов. Из-за особенностей ПЛИС в полученном описании могут встречаться неподсоединенные («висящие») контакты, причем «висящий» контакт у логического элемента означает логическую землю, а «висящий» контакт у триггера – не подсоединенный вход. Поэтому, «висящие» контакты у логических элементов необходимо заменить логическим нулем, а у триггеров – удалить.

Формирователи третьего состояния, на разрешающие входы которых заведен постоянный сигнал, разрешающий прохождение информации через него, должны быть заменены проходными буферами.

Вход логического элемента, на который заведен постоянный сигнал, согласно правилам алгебры логики может быть удален при последующей замене, в случае необходимости (в зависимости от уровня сигнала и функции этого элемента), исходного логического элемента другим элементом. В табл. 1 приведены ТУ таких элементов (исходные ТУ) и соответствующие им ТУ эквивалентных схем (эквивалентные ТУ). Через := обозначена операция присваивания, через $\neg$ –операция инверсии.

Унификация комбинаторных узлов. Для сравнения исходной схемы с полученным описанием необходимо унифицировать в этих описаниях все комбинаторные узлы. Для этого в полученном описании надо: 1) восстановить многовходовые логические элементы, т.е. заменить каждую цепочку одинаковых элементов одним общим элементом; 2) инвертирующие входы и выходы заменить отдельными инверторами.

Эта задача может решаться путем поочередного приложения к описаниям комбинаторных узлов правил замены, приведенных в табл. 2. Они определяют замену каждой исходной цепочки, состоящей из двух логических элементов и описанной ТУ, одним элементом. Символы $\overline{\&}, \overline{\vee}, \overline{\oplus}$ обозначают логические операции, соответственно, И-НЕ, ИЛИ-НЕ, Исключающее ИЛИ-НЕ.

Алгоритм сравнения схем. Сначала необходимо найти соответствие

одинаковых имен внешних цепей в исходном и полученном описаниях, которые не всегда совпадают, так как к исходному имени цепи ***i*** могут добавляться дополнительные обозначения через точку или символ подчеркивания. При сравнении имен цепей это нужно учитывать.

Для сравнения схем предлагается следующий алгоритм:

1. Составить ТУ для исходного и полученного описаний схемы.
2. Удалить из ТУ полученного описания неиспользуемые контакты элементов.
3. Унифицировать комбинаторные узлы исходного и полученного описаний.
4. В ТУ исходного и полученного описаний необходимо выполнить попарную свертку однотипных тензорси, представленных в обоих этих ТУ, начиная с тензорси объектов (ТО), находящихся на уровне w:. Однотипными следует считать тензорси, имеющие одинаковые реляционные знаки (сокращающие символы операций) и одинаковые результирующие переменные.
5. В случае, если в каком-либо ТУ останутся несвернувшиеся тензорси, необходимо сделать вывод о несоответствии двух схем.
6. Исходное и полученное описание схемы можно считать полностью совпадающими только в том случае, если оба эти ТУ свернутся полностью.

Таблица 1.

Исходные ТУ	Эквивалентные ТУ
$\&_{ab}^{q=}\,0$	$:=^{q=}0$
$\&_{ab}^{q=}\,1$	$\&_{ab}^{q=}$
$\vee_{ab}^{q=}\,1$	$:=^{q=}1$
$\vee_{ab}^{q=}\,0$	$\vee_{ab}^{q=}$
$\oplus_{ab}^{q=}\,1$	$\oplus_{ab}^{c}\,\neg_{c}^{q=}$
$\oplus_{ab}^{q=}\,0$	$\oplus_{ab}^{q=}$
$\neg^{q=}0$	$:=^{q=}1$
$\neg^{q=}1$	$:=^{q=}0$

Таблица 2.

Исходное ТУ	Результат Замены
$:=_{b}^{c}:=_{c}^{q=}$	$:=_{b}^{q=}$
$\&_{ab}^{c}\,\&_{cd}^{q=}$	$\&_{abd}^{q=}$
$\vee_{ab}^{c}\,\vee_{cd}^{q=}$	$\vee_{abd}^{q=}$

Продолжение табл. 2.

Исходное ТУ	Результат Замены
$\oplus_{ab}^{c}\,\oplus_{cd}^{q=}$	$\oplus_{abd}^{q=}$
$\neg_{b}^{c}\neg_{c}^{q=}$	$:=_{b}^{q=}$
$\neg_{b}^{c}:=_{c}^{q=}$	$\neg_{b}^{q=}$
$:=_{b}^{c}\,\neg_{c}^{q=}$	$\neg_{b}^{q=}$
$:=_{b}^{c}\,\&_{ac}^{q=}$	$\&_{ab}^{q=}$
$:=_{b}^{c}\,\vee_{ac}^{q=}$	$\vee_{ab}^{q=}$
$:=_{b}^{c}\,\oplus_{ac}^{q=}$	$\oplus_{ab}^{q=}$
$\&_{a\neg b}^{q=}$	$\neg_{b}^{c}\,\&_{ac}^{q=}$
$\vee_{a\neg b}^{q=}$	$\neg_{b}^{c}\,\vee_{ac}^{q=}$
$\oplus_{a\neg b}^{q=}$	$\neg_{b}^{c}\,\oplus_{ac}^{q=}$
$\overline{\&}_{ab}^{q=}$	$\&_{ab}^{c}\,\neg_{c}^{q=}$
$\overline{\vee}_{ab}^{q=}$	$\vee_{ab}^{c}\,\neg_{c}^{q=}$
$\overline{\oplus}_{ab}^{q=}$	$\oplus_{ab}^{c}\,\neg_{c}^{q=}$

Пример контроля схемы на ПЛИС. На рис. 1а приведена исходная схема, которая была выполнена на ПЛИС, а на рис. 1б приведена схема, полученная в процессе проектирования этой ПЛИС.

В полученную схему САПР ПЛИС внесла цепь сброса по питанию g, невидимую для разработчика при вводе схемы, а также разбила логический элемент ИЛИ-НЕ на два отдельных элемента – дизъюнктор и инвертор.

Контакты S и CE в полученной схеме являются «висящими». Выполним сравнение исходной и полученной схем согласно приведенному алгоритму.

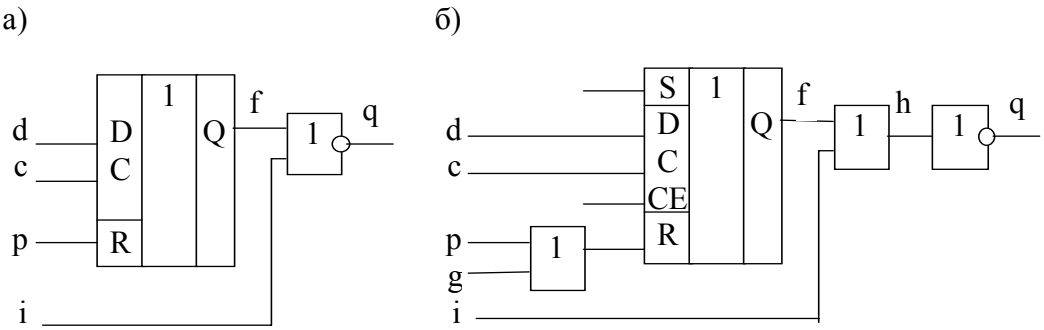


Рис. 1. Пример схемы, выполненной на ПЛИС:
а) исходная схема; б) полученная схема.

Тензорное уравнение исходной схемы будет иметь следующий вид:

$$e^d e^c e^p e^i T_{\Gamma} D^f_{pcd} \overline{\vee}^q_{fi} e^q \qquad (1)$$

Тензорное уравнение полученной схемы будет иметь вид:

$$e^d e^c e^p e^i e^g \vee^x_{pg} T_{\Gamma} D^f_{xcd} \vee^h_{fi} \neg^q_h e^q \qquad (2)$$

Из выражения (2) уже удалены «висящие» контакты триггера. Поскольку других неиспользуемых контактов в схеме рис. 1 нет, то далее следует провести унификацию логических элементов в схеме.

Элемент ИЛИ-НЕ, присутствующий в выражении (1), необходимо разделить на дизъюнктор и инвертор. В результате ТУ исходной схемы примет вид:

$$e^d e^c e^p e^i T_{\Gamma} D^f_{pcd} \vee^b_{fi} \neg^q_b e^q \qquad (3)$$

Цепь *b* внесена в ТУ (3) произвольно.

Согласно п. 4 алгоритма сравнения схем для ТУ (3) и ТУ (2) необходимо выполнить свертку однотипных тензорси, начиная с ТО e^q. При этом ТУ (3) свернется полностью, а в ТУ (2) останутся тензорси, описывающие цепь дополнительного сброса по питанию:

$$e^g \vee^x_{pg} \qquad (4)$$

Таким образом, в результате сравнения приведенных на рис. 1 разновидностей одной схемы выявлено их несоответствие, которое заключается в том, что в полученное описание добавлена дополнительная цепь. В данном случае такая «добавка» в полученном описании схемы не оказывает влияния на правильность ее работы. В других случаях подобные дополнительные узлы могут быть как непреднамеренными ошибками, так и преднамеренными закладками.

Заключение. В настоящей работе предложена методика контроля соответствия полученной схемы, выполненной на ПЛИС, описанию исходной схемы, позволяющая: 1) выявлять лишние элементы, внесенные в схему в процессе ее преобразования; 2) находить и выделять несоответствия между исходной и полученной схемами.

Литература

1. Чижухин Г.Н. Тензорная алгебраическая система. // Новые информационные технологии и системы: Труды V Международной научно-технической конференции. – Пенза, ПГУ, 2002. – с. 195 – 202.

Получено 29.10.2003. Доклад опубликован в Internet 2.11.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.60-63. Секция-4: Анализ вычислительной среды, верификация, сертификация программ.
Пенза-август-2002 (http://beda.stup.ac.ru/RV-conf/v04/014)

АНАЛИЗ ВРЕМЕННЫХ ПАРАМЕТРОВ СХЕМ БЕЗ ИСПОЛЬЗОВАНИЯ МОДЕЛИРОВАНИЯ

Кулагин О.В.
Пензенский научно-исследовательский электротехнический институт

Введение. После выполнения любой электрической схемы на ПЛИС необходимо убедиться в том, что получившиеся задержки распространения сигналов не искажают алгоритм работы схемы, и что этот алгоритм полностью соответствует исходному. Задержки и вызванные ими риски сбоя в схеме обычно анализируются при помощи моделирования [1-4], заключающегося в формировании выходных сигналов схемы на предварительно определенных тестовых наборах. Однако, очень сложно составить тестовые наборы, полностью определяющие работоспособность больших схем, а моделирование таких схем весьма громоздко. Поэтому, необходим способ анализа временных параметров схем без использования моделирования.

Синхронные и асинхронные схемы. Все цифровые схемы могут быть поделены на два класса – синхронные и асинхронные. Асинхронные схемы способны воспринимать входные сигналы и формировать соответствующие им выходные сигналы в любой момент времени. Синхронные схемы наоборот, воспринимают входные сигналы только в определенные моменты времени, задаваемые синхросигналом. После прихода синхроимпульса в схеме сначала возникают переходные процессы, вызванные изменением в ней значений сигналов, потом формируются истинные значения выходных сигналов, и далее схема простаивает до прихода следующего синхроимпульса. Поэтому, если переходные процессы заканчиваются до нового переключения схемы, то она будет работать без сбоев.

Асинхронными элементами являются все виды комбинаторных логических элементов и асинхронные триггеры (например, RS-триггеры), синхронными – синхронизируемые триггеры, защелки, регистры хранения, ОЗУ, ПЗУ и формирователи третьего состояния. Остальные электрические элементы, например счетчики и сдвиговые регистры, являются комбинациями регистров хранения и комбинаторных узлов, т.е. фактически это отдельные схемы, а не элементы. Схема является синхронной, если в ней имеется хотя бы один синхронный элемент, и асинхронной в противном случае.

Временные диаграммы логических элементов. На рисунке 1 показаны временные диаграммы двухвходовых логических элементов – дизъюнктора, конъюнктора, сумматора по модулю два, причем на рис. 1а оба входных сигнала – a и b – переключаются одновременно, без задержек; на рис. 1б сигнал a имеет задержку τ относительно сигнала b; на рис. 1в наоборот, сигнал b имеет задержку τ относительно сигнала a.

На рисунке 1 на входах логических элементов перебираются все возможные двухвходовые кодовые комбинации. Порядок их следования подобран так, чтобы риски сбоя на рис. 1б и 1в были заметнее. Для этого в моменты времени **T**, соответствующие длительности каждой кодовой комбинации и помеченные на рис. 1 пунктирными линиями, меняются, по возможности, оба

входных сигнала. Штрихпунктирными линиями на рис. 1б и 1в помечены моменты времени τ.

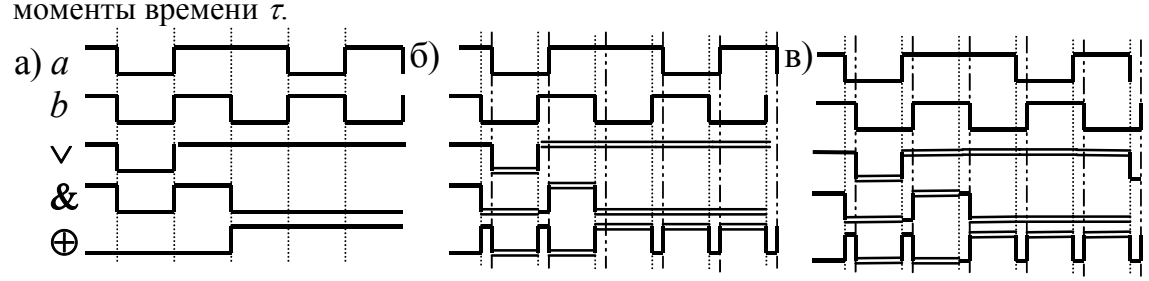


Рис. 1. Временные диаграммы логических элементов: а) при отсутствии задержек; б) при задержке сигнала *a*; в) при задержке сигнала *b*.

На основе сравнения рис. 1а, 1б и 1в можно сделать вывод, что выходные сигналы искажаются только на временных интервалах [**0**, τ], а на интервалах [τ, **T**] все выходные сигналы имеют свои истинные значения, обозначенные двойными линиями. Моделирование схемы с использованием n тестовых векторов, каждый из которых имеет длительность **T,** на временном интервале [**0**, n**T**] можно заменить временным анализом на интервале [**0**, **T**] при соблюдении условий: 1) входная комбинация любого комбинаторного узла цифровой электрической схемы удерживается на его входах в течение времени **T**; 2) переходные процессы в схеме после переключения сигналов занимают интервалы [**0**, τ]; 3) τ<**T**/2; 4) все сигналы в схеме записываются в элементы памяти только на интервалах [τ, **T**].

Информация на входы комбинаторных узлов схемы может поступать либо со входных контактов, на которых каждая входная комбинация имеет длительность **T**, либо с выходов элементов памяти схемы по некоторому сигналу чтения. Так как сигнал чтения определяет наличие информации на выходе элемента в течение всего временного интервала [**0**, **T**], то он должен иметь активный уровень на всем этом интервале. Сигнал записи должен обеспечивать запись информации на интервале [τ, **T**] либо по фронту, либо по уровню. Временные диаграммы разрешающих и информационных сигналов приведены на рис. 2а, где запись информации можно производить либо по положительному фронту (от нуля к единице), либо по низкому уровню.

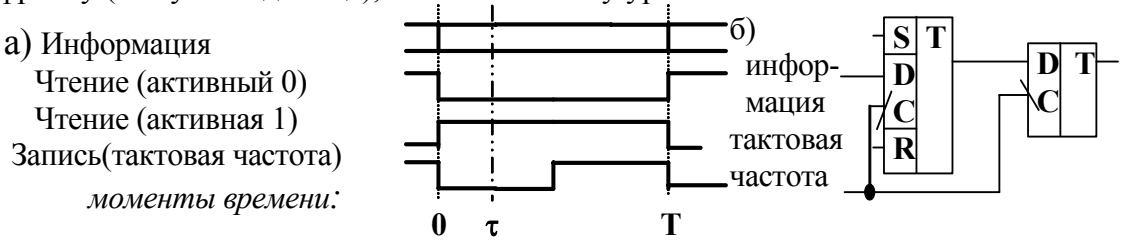


Рис. 2. а) временные диаграммы информационных и разрешающих сигналов; б) двухтриггерная схема, имеющая эту диаграмму.

При соблюдении приведенных на рис. 2а соотношений для информационных и разрешающих сигналов для каждого синхронного элемента, все сигналы в схеме будут фиксироваться правильно. Однако, на выходах элементов памяти, не имеющих третьего состояния (например, триггерах), по истечение некоторого времени $t_{ср}$ (которое равно задержке между моментом записи новой информации в триггер и моментом появления этой информации на его выходе, и которое назовем временем срабатывания элемента) после записи информации появятся новые значения сигналов, которые могут исказить входные сигналы для еще не сработавших триггеров схемы. Поэтому, выходные сигналы

всех триггеров (элементов памяти) схемы необходимо держать неизменными до наступления момента времени **T**, а для этого вместо одиночных триггеров в схеме необходимо использовать двухтриггерную схему (триггер с динамическим управлением), показанную на рис. 2б. При асинхронном сбросе или установке первого триггера, либо по положительному перепаду тактовой частоты, новая информация будет записана в первый триггер, но на выходе второго триггера старая информация будет храниться до наступления момента времени **T**, в который информация с выхода первого триггера перепишется во второй. Таким образом, будет соблюдено соотношение рис. 2а для всех элементов памяти схемы и исключены ложные срабатывания из-за разброса задержек сигналов.

Временной анализ на интервале [**0**, **T**] необходимо проводить в два этапа: 1) нахождение тактовой частоты схемы; и 2) проверка правильности записи информации в элементы памяти схемы. На первом этапе подсчитывается величина максимальной тактовой частоты, на которой схема будет работать без сбоев, а на втором проверяется влияние разброса задержек схемы на запись информации в ее элементы памяти.

Нахождение тактовой частоты схемы. Начинать временной анализ на интервале [**0**, **T**] необходимо с получения файла САПР ПЛИС, содержащего описания полностью готовой схемы с временными задержками. Далее необходимо сделать следующее:

1. Разделить схему на синхронные и асинхронные (комбинаторные) узлы.
2. Определить максимальную задержку распространения сигналов в комбинаторных узлах схемы $t_к = \max(t_{к1}, t_{к2},..., t_{кm})$, где m – количество комбинаторных узлов в схеме, $t_{кi}$ – задержка распространения сигналов в ***i***-м комбинаторном узле $t_{кi} = \max(t_{i1}, t_{i2},..., t_{in})$, n – количество входов в *i*-м узле; t_{i1}, t_{i2},..., t_{in} – задержки распространения сигналов от соответствующего входа *i*-го узла до его выхода.
3. Время окончания переходных процессов в схеме $\tau = t_к$.
4. Так как $\tau < \mathbf{T}/2$, то справедливо равенство $\mathbf{T} = 2(\tau+\Delta\tau)$, где $\Delta\tau$ – заранее определенная временная константа, гарантирующая выполнение указанного неравенства. Так находится период тактовой частоты, на которой схема будет работать без сбоев.

Проверка правильности записи информации в элементы памяти схемы. Из-за разброса задержек синхросигналов в цепочке последовательно соединенных триггеров последующие триггеры могут переключаться после записи новых значений в предыдущие триггеры. В этом случае из предшествующих триггеров в последующие вместо требуемых значений будут записаны новые значения. Такую ситуацию можно избежать двумя способами: 1) минимизацией задержек синхросигналов, например, за счет их передачи по специальным цепям с низкой задержкой, которые в ПЛИС фирмы Xilinx названы *глобальными*; 2) применением вместо обычных триггеров двухтриггерных схем рис. 2б для тех ПЛИС, в которых глобальных цепей нет.

Проверять правильность записи информации в элементы памяти схемы необходимо следующим образом:

1. Для всех синхронных элементов схемы нужно определить временной интервал внутри отрезка [**0**, **T**], на котором их синхросигналы имеют активные значения. Сигналы чтения будут активны на всем этом интервале [**0**, **T**], сигналы записи с активным низким уровнем – на временном интервале [**0**, **T**/2], сигналы записи с активным передним (положительным) фронтом – в момент времени **T**/2, а сигналы записи с активным задним (отрицательным) фронтом – в

момент времени 0. Итак, для сигналов с активными уровнями это будут временные интервалы [**0**, *t*], где величина *t* может принимать значение **T** или **T**/2, а для сигналов с активными фронтами – одиночные моменты времени $t_ф$ ($t_ф$ принимает значения **0** или **T**/2).

2. Для каждого синхронного элемента, синхросигналы которых имеют активные фронты, необходимо определить интервал, в течение которого происходить запись информации в этот элемент (назовем данный интервал *интервалом записи*) – промежуток времени $[t_c+t_ф, t_c+t_ф+t_{ср}]$, в течение которого в схеме происходит запись информации. Через t_c обозначена задержка синхросигнала.

3. Для каждого комбинаторного узла схемы необходимо определить интервал, в течение которого происходят изменения его входных сигналов (назовем этот интервал *интервалом изменения*). Если на некоторые входы этого узла подключены выходы триггеров, то из их числа необходимо выбрать триггер с минимальной задержкой синхросигнала t_cmin и триггер с максимальной задержкой синхросигнала t_cmax. Тогда началом интервала изменения будет момент времени $t_cmin+t_ф+t_{ср}+ t_cmax–t_cmin$, а концом – момент времени $t_K+t_cmin+t_ф+t_{ср}+t_cmax–t_cmin$. Для всех одинаковых элементов одной ПЛИС величина $t_{ср}$ будет постоянной. Если к одному комбинаторному узлу подключены триггеры (или другие синхронные элементы) с разными $t_ф$, интервал изменения для такого узла будет представлять собой объединение интервалов изменения, найденных для всех этих значений $t_ф$.

4. Если интервал записи не будет перекрываться с интервалом изменения, то схема будет работать правильно. В противном случае схема будет неработоспособной.

Для исправления неработоспособной схемы необходимо либо завести все ее синхросигналы на глобальные цепи, либо заменить все одиночные триггеры в этой схеме на двухтриггерные схемы. Подтвердить правильность исправлений в схеме поможет ее повторный временной анализ на интервале [**0**, **T**].

Заключение. В работе предложена методика проведения временного анализа схемы на интервале [**0**, **T**], позволяющая для этой схемы: 1) исключить моделирование из процесса анализа временных параметров; 2) определить величину тактовой частоты; 3) определить правильность записи информации в элементы памяти.

Литература

5. Воробьев Н. Риски сбоя в комбинационных схемах. // ChipNews, 1998, № 2. – с. 26-30.
6. Воробьев Н. Методы анализа комбинационных схем на риски сбоя. // ChipNews, 1998, № 3. – с. 42-44.
7. Воробьев Н. Рекомендации по устранению рисков сбоя в комбинационных схемах. // ChipNews, 1998, № 4. – с. 47-49.
8. Левин В.И. Динамика логических устройств и систем. – М.: Энергия, 1980.

Получено 29.10.2003. Доклад опубликован в Internet 2.11.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.64-67. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/015)

ПАКЕТ ЛАБОРАТОРНЫХ РАБОТ ПО НЕЙРОСЕТЕВОМУ АНАЛИЗУ ДИНАМИКИ РУКОПИСНОГО ПОЧЕРКА

Капитуров Н.В., Иванов А.И., Глухов Д.Н.
Лаборатория биометрических и нейросетевых технологий
Пензенского научно-исследовательского электротехнического института,
Пензенский государственный университет

Объединение технологий высоконадежной биометрической аутентификации, нейросетевой обработки и криптографической защиты информации делает возможным создание нового поколения электронных денег, электронных паспортов, удостоверений личности. Новое поколение электронных документов (всемирных денег, паспортов, удостоверений личности) по прогнозам экспертов должно быть инвариантно к вычислительной среде, не будет иметь физического носителя, ими можно будет пользоваться находясь на любом удалении не прибегая к специальным устройствам и специальным носителям секретов.

Очевидно, что криптографические технологии поддержания безопасности электронных документов нового типа достаточно хорошо развиты и обеспечены высококвалифицированными специалистами. Иначе обстоит дело с биометрическими и нейросетевыми технологиями. На сегодняшний день специалистов по биометрии в России не готовят. Нет так же подготовки специалистов одновременно владеющих особенностями биометрических технологий в совокупности с особенностями создания и обучения больших нейронных сетей, способных принимать решения высокой надежности. Биометрико-нейросетевые технологии защиты будущих электронных денег и электронных документов должны обеспечивать вероятность случайной ошибки на уровне $10^{-20}…10^{-40}$ сопоставимую с вероятность взлома криптографической защиты при случайном подборе ключа. В связи со сложностью таких задач и высокой ответственностью при их реализации необходимо заранее начинать подготовку высококвалифицированных специалистов одновременно владеющих биометрией и нейроинформатикой.

Сравнительный анализ проблем преподавания биометрии и нейроинформатики показал, что студенты инженерных специальностей на много проще воспринимают биометрические технологии в сравнением с нейросетевыми. Биометрические технологии имеют хорошую опору на математическую статистику и ряд других классических инженерных дисциплин. Иначе обстоит дело с нейросетевыми технологиями, которые имеют слабое теоретическое обоснование и потому должны быть усилены практическими занятиями (лабораторными работами), позволяющими каждому студенту убедится в возможности обучения искусственных нейронных сетей.

При практическом использовании искусственных нейронных сетей не так важно знать теорию их синтеза и обучения, как иметь практические навыки по обучению реальных нейронных сетей. Студент должен почувствовать, что в процессе обучения искусственных нейронных сетей существуют реальные тупики, попав в этот тупик далее двигаться нельзя. Например, из-за плохого качества входных данных, недостаточного количества примеров, противоречивости примеров, недостаточной сложности нейронной сети (мало слоев нейронов, мало связей нейронов, мало самих нейронов в слое), неправильно заданной конфигурации нейронной сети, не верно выбранной концепции обучения.

Как показал опыт все эти проблемы легко понимаются всеми людьми на интуитивном уровне, опирающимся на практический опыт обучения нейронных сетей. Как следствие преподавание теории искусственных нейронных сетей должно быть подкреплено достаточно объемным курсом практических работ, который должен

позволить студентам получить подсознательные навыки по решению этого типа задач. Видимо, при преподавании нейроинформатики по аналогии с курсами вождения автомобиля необходимо вырабатывать у студентов практические навыки и учить их ощущать попадание при обучении нейронных сетей в тот или иной тупик обучения. Люди способны очень быстро обучаться на интуитивном уровне и это очень важно, особенно в тех случаях, когда теория предмета еще достаточно слабо развита.

В связи с вышеизложенным Пензенский государственный университет совместно с «Лабораторией биометрических и нейросетевых технологий» Пензенского научно-исследовательского электротехнического института приступили к созданию курса лабораторных работ по нейроинформатике.

Курс лабораторных работ строится на распознавании рукописных символов, вводимых студентами через стандартный графический планшет или если нет планшета, то используется стандартный манипулятор «мышь». Студенты вводят своим почерком рукописные буквы как это показано на рисунке 1.

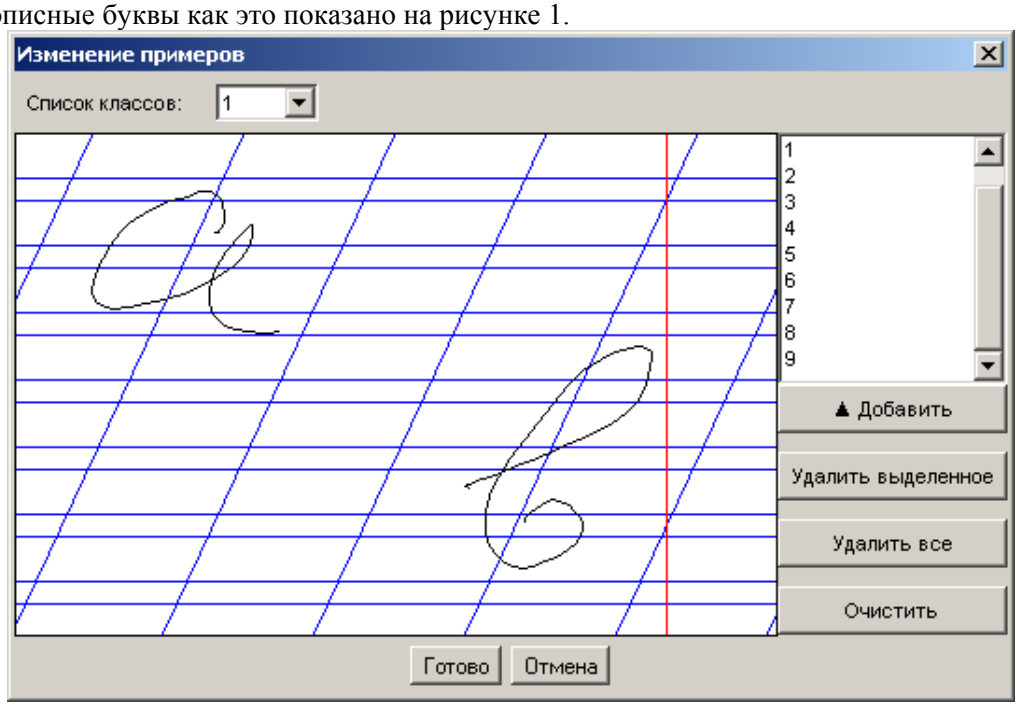


Рисунок 1. Окно отображения вводимых примеров рукописной графики, используемых далее при обучении или тестировании нейросети.

Предусматривается порядка 20 различных лабораторных работ по изучению влияния:

- числа учитываемых нейронной сетью параметров;
- качества учитываемых нейронной сетью параметров;
- числа слоев нейронов в нейросети,
- числе нейронов в нейросети,
- числа входов у каждого нейрона,
- вида функций возбуждения.

Обучение и тестирование нейронных сетей поддерживается графикой, отражающей реальные гистограммы распределения значений выходных данных и их аппроксимацию нормальными законами распределения значений. На рисунке 2 приведен пример подобной аппроксимации для нейросети с одним выходом и нечетной выходной нелинейностью предназначенной для разделения двух классов (для класса образов «*а*» - индексы – 1, для класса образов «*в*» - индексы – 2,). Графика примеров разделяемых классов «*а*» и «*в*» дана на рисунке 1.

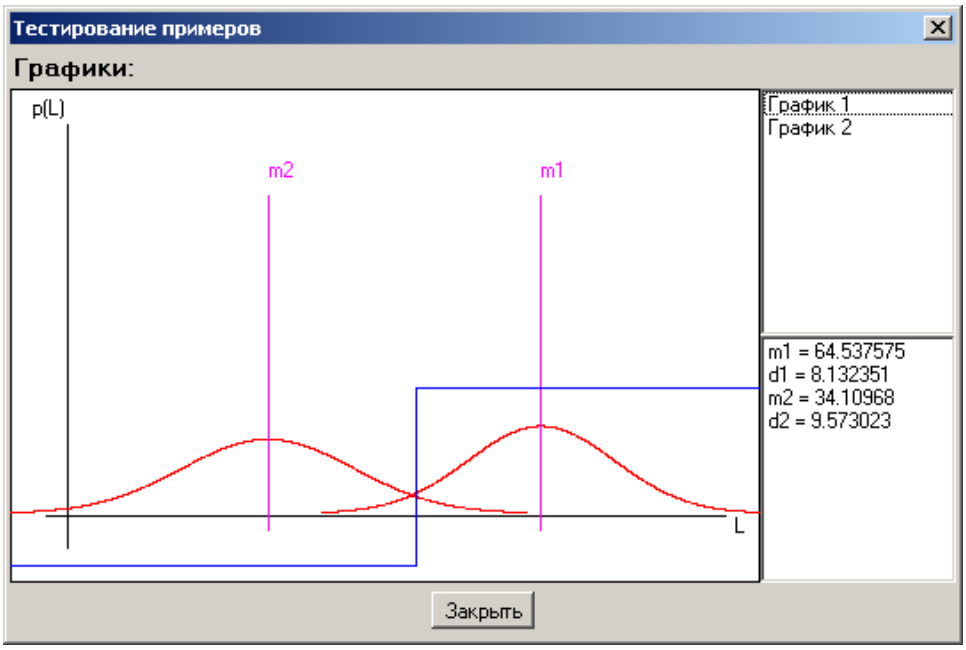


Рисунок 2. Пример разделения двух классов «*а*» и «*в*» нечетной нелинейной функцией на выходе одного нейрона с 16 входами.

На рисунке 3 дан пример плотностей распределений значений на одном из выходов более сложной нейронной сети, состоящей из 4 нейронов и предназначенной для выделения 4 различных графических образов «*а*», «*б*», «*с*», «*d*». В простейшем случае эта сеть должна иметь 4 выхода и на каждом выходе содержать четный нелинейный элемент.

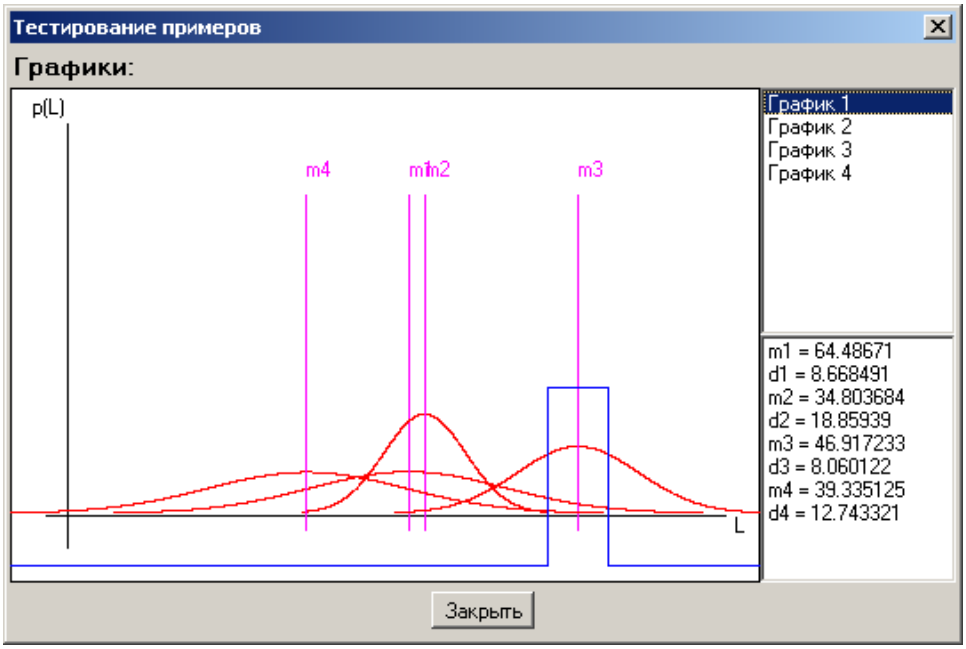


Рисунок 3. Пример распределения на одном из выходов нейронной сети предназначенной для выделения образов 4 разных классов

Влияние качества данных на процесс обучения нейронных сетей проверяется в двух режимах. В режиме использования для ввода информации графического планшета получается высокое разрешение (графический образ одной буквы содержит порядка 100 отсчетов координат положений конца пера при рукописном воспроизведении буквы). При переходе к использованию в место графического планшета манипулятора «мышь» число отсчетов, приходящихся на один графический образ резко падает, что и дает

возможность снизить качество входных данных и проследить его влияние на процесс обучения нейросети.

Кроме изменения качества данных в программном продукте предусмотрен режим изменения числа учитываемых параметров. Предусмотрено использование до 96 контролируемых нейронной сетью параметров. Реально учитываемое число параметров задается в специальном диалоговом окне. В этом же окне задается число выходов нейросети, число слоев нейросети, число входов у нейронов и вид их функции возбуждения.

Программное обеспечение написано на языке JAVA, ориентировано на работу под ОС Windows 98/2000/NT/XP. Пакет состоит из 6 программных модулей, связь между которыми отображена на рисунке 4.

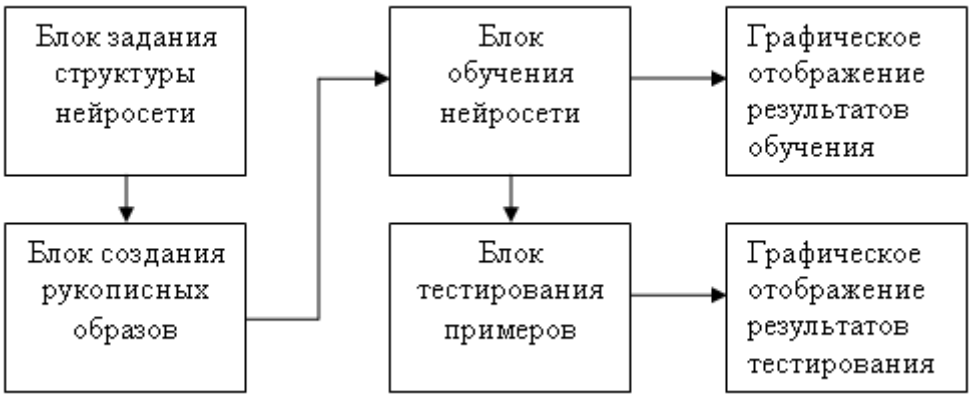


Рисунок 4. Структурная блок-схема программного обеспечения пакета лабораторных работ

Пробная эксплуатация пакета программ намечена на первый квартал 2004 года в рамках курса «Нейросети», читаемого в Пензенском государственном университете на кафедре «Информационная безопасность систем и технологий».

Получено 30.10.2003. Доклад опубликован в Internet 4.11.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.68-70. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/016)

ПРОТИВОРДЕЙСТВИЕ НЕЗАКОННОЙ ДОБЫЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИИ ИЗ МАССИВОВ ДЕЛОВЫХ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Ефимов О.В.
Пензенский научно-исследовательский электротехнический институт

Сегодня традиционные денежные системы, системы торговли и документооборота постепенно вытесняются электронными системами. В результате внедрения таких систем кроме очевидных положительных эффектов создаются предпосылки по автоматическому сбору (перехвату) и накоплению злоумышленниками огромных объемов открытой достоверной информации. Дело в том, что в любой открытой достоверной информации размыта конфиденциальная информация. Порою лица, ведущие деловую переписку, даже не подозревают о том, что формируют пласты богатой информации достаточно удобной для последующего извлечения из нее конфиденциальных данных. Используя современные поисковые машины и машины добычи (обогащения) данных удается извлекать из несекретной информации ее конфиденциальные составляющие знаний. Вопрос состоит только в получении злоумышленником необходимых объемов достоверной исходной сырьевой информации и качестве поисковых машин, а также машин обогащения данных. При этом нужно иметь в виду, что технологии создания поисковых машин и машин извлечения знаний быстро развиваются. То, что было невозможно вчера, становится реальным сегодня. Создавая системы защиты информационного пространства России и системы активного информационного противодействия необходимо ориентироваться на перспективу, чтобы разрабатываемые системы оставались эффективными как минимум 10-15 лет после их запуска.

Одним из путей защиты информационного пространства России является массовое использование криптографической защиты, как при ведении деловой электронной переписки между государственными (муниципальными) предприятиями и учреждениями, экономически значимыми частными коммерческими структурами, так и при ведении деловой переписки между их сотрудниками, находящимися вне предприятия. При этом система защиты не должна мешать пользователям, затрудняя их работу. Система должна быть дружественной к пользователям, криптографические механизмы защиты должны быть невидимыми для пользователей. Стойкость защиты может быть не очень высокой, но она должна быть тотальной и невидимой для легитимных пользователей. Ее цель – защита открытой информации от автоматизированного нелегального перехвата и накопления значительных массивов данных (больше некоторого критического объема). Однако при массовом использовании криптографии возникает проблема хранения личных ключей миллионов пользователей. Эту задачу не удается решить традиционными методами.

Поскольку длина ключей велика и превышает возможности памяти обычного человека, ключи записываются на какой-либо физический носитель – бумага, дискета, пластиковая карточка и т.д. В отличие от традиционных систем для «взлома» электронных систем необязательно украсть ключ – достаточно его скопировать. Факт копирования ключа установить чрезвычайно сложно и, следовательно, о преодолении системы защиты чаще всего мы узнаем только

после нанесения ущерба. Традиционные способы сохранения ключей в тайне - сейфы, вооруженная охрана, 1-ые отделы и др. - не применимы для массового использования.

Таким образом, при широком внедрении систем электронного документооборота, электронной коммерции, электронных паспортов, электронных денег и других информационно-телекоммуникационных систем одной из наиболее острых проблем будет создание новых технологий и массовых средств защиты, направленных на противодействие добыче из множества достоверной открытой информации критических секретов, влияющих на безопасность как отдельных хозяйствующих субъектов, так и на безопасность органов власти и управления России в целом.

Сегодня решение проблемы создания массовых средств по противодействию добыче знаний (секретов) видится в соединении криптографических, биометрических и нейросетевых технологий. В самом деле, биометрические характеристики каждого человека уникальны и в совокупности не поддаются подделке, их невозможно, потерять и подчас очень трудно копировать. Они всегда под рукой и потому очень удобны. Задача состоит лишь в том, чтобы научиться их измерять простыми и дешевыми методами с достаточной точностью и использовать для криптографических преобразований – шифрования и электронной цифровой подписи. Теоретические подходы к решению этой задачи уже найдены, сегодня в ПНИЭИ ведутся работы по их практической апробации, по совершенствованию методов измерения биометрических характеристик и методов их преобразования в криптографические ключи [1].

Мировая научно-техническая общественность, официальная позиция которой выражена в официальных документах международного технического комитета ISO/IEC JTC 1/CS27 и ISO/IEC JTC 1/CS37, признает, что контроль достоверности массового электронного документооборота, безопасность электронного денежного обращения (электронной Internet коммерции), дистанционное управление сложными объектами можно сделать безопасным только с применением средств биометрии и криптографии. Однако предлагаемые биометрические системы защиты решают только задачу определения «Свой»/«Чужой», работают в отрыве от криптографии, используют дорогие и не очень надежно защищенные от подделки открытые статические биометрические образы - отпечатки пальцев, сетчатка глаза, геометрия лица, руки и др.

Отечественные ученые предлагают наряду с открытыми использовать тайные биометрические образы [2], которые крайне сложно подделать – это динамические особенности рукописного почерка, особенности голоса, виброаккустические особенности строения костно-мышечных тканей. При этом средства измерения биометрических характеристик человека очень дешевы и применяются повсеместно – микрофон, ларингофон, графический планшет, компьютерная мышь.

Сегодня в ПНИЭИ ведутся работы по созданию хранителей личных секретов [1], которые могут быть положены в основу технологии и технических средств противодействия добыче знаний (секретов). В них применяются алгоритмы быстрого обучения искусственных нейронных сетей мировой новизны, а также программы измерения биометрических характеристик рукописного почерка. Ожидается, что технико-экономические характеристики разрабатываемой продукции будут существенно превышать мировой уровень. Однако уникальность и принципиальная новизна такой продукции не позволяют оценить возможность ее применения в столь ответственной сфере, как информационная безопасность государства. Требуется проведение работ не

только по совмещению биометрических, нейросетевых и криптографических технологий, но и разработка технологий по выявлению технических характеристик средств противодействия добыче знаний, их сертификации, а также по определению мест установки и порядка использования средств противодействия в существующих и будущих информационно-телекоммуникационных системах.

Работы проводимые в ПНИЭИ показали, что одним из самых эффективных мест применения биометрической аутентификации является организация доступа к ИНТЕРНЕТ на государственном предприятии [3] и организация защиты трафика исходящей с предприятия электронной почты. Предполагается, что должна быть создана личная почтовая программа для каждого работника предприятия, которая способна узнавать своего хозяина и обеспечивать защиту связи электронной почтой работника предприятия с почтовым сервером предприятия. При этом работник предприятия не ощущает никаких затруднений при пользовании программой, он не ощущает, трафик его переписки защищен.

ЛИТЕРАТУРА

1. Ефимов О.В., Иванов А.И. Программные хранители паролей с биометрическим доступом. //Современные технологии безопасности 2002, № 2., с. 30-22.
2. Глухов Д.Н., Иванов А.И. Оценка стойкости тайных биометрических образов человека //Современные технологии безопасности 2003, № 2(5)., с. 30-32.
3. Ефимов О.В. О подключении режимных предприятий к сети ИНТЕРНЕТ. //Современные технологии безопасности 2002, № 3., с. 23-25.

Получено 10.11.2003. Доклад опубликован в Internet 14.11.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.71-72. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/017)

СИСТЕМА КОНТРОЛЯ ИСХОДЯЩЕЙ ЭЛЕКТРОННОЙ ПОЧТЫ «НИПЕЛЬ 2002»

Мигин В.И., Ефимов О.В., Иванов А.И.
Пензенский научно-исследовательский электротехнический институт

Система предназначена для контроля ВСЕЙ исходящей электронной почты пред-приятия работниками отде-лов безопасности в соот-ветствии с требованиями Российского законодатель-ства. Система позволяет заводить ВСЕМ работни-кам предприятия личные почтовые адреса на почтовом сервере пред-приятия и тем самым сократить сроки деловой переписки с другими организациями, снизить затраты на междугородние телефонные переговоры. Срок окупаемости системы 6 месяцев для предприятия с численностью 1000 человек. Входной трафик электронной почты не контролируется.

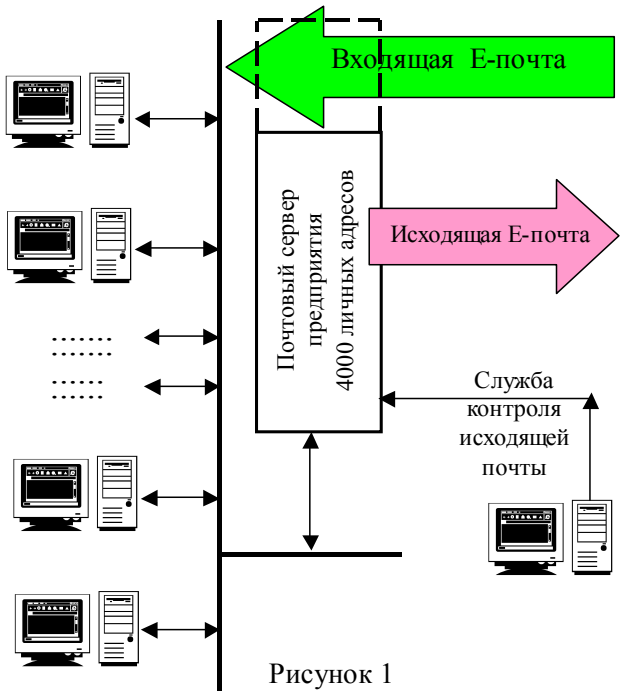


Рисунок 1

Система «Нипель-2002» обеспечивает:

- возможность организации до 4000 личных адресов электронной почты служащих;
- практически полный контроль исходящей электронной почты (вероятность пропуска электронной почты через чужой почтовый русскоязычный сервер менее 0,001);
- прием входящей электронной почты без задержки;
- задержка исходящей электронной почты на контроль не более 2 часов;
- сообщение работнику об отправке его электронной почты с сервера предприятия.

В настоящее время большие госпредприятия России имеют всего 1 или 2 официальных адреса электронной почты. Это приводит к ощутимым задержкам доставки электронной почты. Работники предприятия зачастую вынуждены нарушать принятый порядок и пользоваться для деловой переписки сторонними почтовыми серверами (www.mail.ru, mail.yandex.ru,…) минуя обязательный контроль ВСЕХ исходящих с предприятия писем. За такого типа нарушения несут ответственность как работник предприятия, так и директор предприятия.

Предлагаемая система «Нипель-2002» позволяет дать каждому работнику предприятия личный почтовый адрес для ведения им деловой переписки одновременно выполнив требование Российского законодательства по контролю содержания всех исходящих с предприятия писем.

Долгое время (в плоть до ноября 2002 года) у Пензенского научно-исследовательского института был единственный ящик электронной почты, что приводило к задержкам в доставке деловой почты к конкретным сотрудникам. Почтовый ящик просматривался два раза за рабочий день, далее проводилась распечатка информации, ее переадресовка и доставка внутри предприятия через канцелярию. В неблагоприятные моменты (приход электронной почты в конце рабочего дня предшествующего выходным или праздникам) задержка получения электронной почты исполнителями внутри предприятия могла составить несколько суток (особенно, если далее следовали многодневные праздники), что отрицательно сказывалось на длительности деловых переговоров и процессов уточнения технических деталей при работе со сторонними организациями.

В связи с этим в ноябре 2002 года бала введена система КОНТРОЛЯ ИСХОДЯЩЕЙ ЭЛЕНТОННОЙ ПОЧТЫ «НИПЕЛЬ 2002», которая позволила всем ведущим специалистам предприятия завести свой ящик для электронной почты. Структурная схема системы приведена на рисунке 1. Система построена таким образом, что бы пользователи минимально ощущали контроль исходящей корреспонденции, организованный на предприятии.

Все пользователи сети предприятия пользуются для получения и отправки электронной почты обычными почтовыми программами. Входной почтовый трафик передается пользователям без контроля. Контролируются только исходящие с предприятия письма. Эти письма попадают на почтовый сервер предприятия и отправляются только по команде с рабочего места службы безопасности после их просмотра. При этом отправитель почты оповещается об ее отправке.

Полуторогодовая эксплуатация системы показала, что часть работников предприятия оказались несознательными и пытались пользоваться для электронной переписки «чужими» почтовыми серверами, минуя почтовый сервер своего предприятия. В этих ситуациях система «Нипель» идентифицирует «чужой» почтовый сервер и дает сообщение пользователю-нарушителю о недопустимости его поведения. Как правило этого оказывается достаточно и пользователь отказывается от попытки отправки электронной почты в обход контролируемого почтового сервера предприятия.

В данный момент установлен запрет на работу пользователей через любой сторонний почтовый сервер [1], однако система может быть доработана для возможности отправки с предприятия коротких SMS сообщений на мобильные телефоны, через почтовые сервера провайдеров мобильной связи. Основным отличием системы «Нипель 2002» от ее зарубежных аналогов [2] является то, что она полностью соответствует требованиям Российского законодательства по полному контролю всей исходящей почты с предприятия.

Литература:

1. Ефимов О.В. О подключении режимных предприятий к сети Интернет. Современные технологии безопасности. №3, 2002 г., с23-24.

2. Александр Прохоров Системы клиент-секьюрити на страже корпоративных интересов. КопьютерПресс № 9, 2003, с.160-162.

Получено 10.11.2003. Доклад опубликован в Internet 14.11.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.73-77. Секция-8: Конфиденциальность, целостность, доступность.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/018)

ЗАЩИТА ВИДЕОКОНФЕРЕНЦИЙ В КОРПОРАТИВНЫХ СЕТЯХ СВЯЗИ

Фунтиков Д.А.
Филиал ПНИЭИ - НИП "Аргус"

Введение

Вопросы, связанные с защитой информации в сетях видеоконференцсвязи часто становятся очень актуальными. При этом необходимо помнить, что согласно законодательству Российской Федерации, в качестве средств защиты информации могут использоваться только сертифицированные средства, что обуславливает необходимость применения отечественного оборудования.

Видеоконференцсвязь (ВКС) может быть двухсторонней и групповой.

При двухсторонней ВКС терминальное оборудование взаимодействует между собой напрямую, в качестве транспортной сети может быть использована сеть ISDN или IP. Скорость передачи по линиям ISDN может колебаться от 128 да 512 кбит/с, при этом используются от одного до четырех интерфейсов BRI соответственно. В IP-сетях скорость передачи может достигать 2Мбит/с. Как правило, оборудование ВКС поддерживает стандарты H.320 для сети ISDN и H.323 для сетей IP, что позволяет организовывать групповые сеансы ВКС.

Групповые системы видеоконференцсвязи можно использовать при проведении как больших, так и небольших по количеству участников видеоконференций. Для проведения сеансов ВКС с участием нескольких абонентов (3 и более), применяется специализированное устройство - сервер управления многоточечными сеансами (Multipoint Control Unit -- MCU) ВКС.

Современные MCU являются достаточно универсальными устройствами. Они обеспечивают работу с телефонными станциями и оконечным оборудованием любых производителей придерживающих стандарты ITU-T. Набор сетевых интерфейсов (E1, T1, V.35, RS449, BRI или PRI ISDN, Ethernet) позволяет одновременно участвовать в конференции широкому кругу абонентов. Возможно добавление к текущей видеоконференции участников из аналоговой телефонной сети и сети передачи данных IP, проведение конференций "аудио", "аудио-данные" и "видео-аудио-данные". Большинство современных MCU, имеют открытую архитектуру, поэтому чтобы добавить новую функцию к существующей системе, достаточно установить дополнительную плату и программное обеспечение.

Защита видеоконференцсвязи в сетях ISDN

Учитывая, что информация, передаваемая в сеансах видеоконференцсвязи, может содержать конфиденциальные сведения, необходимо обеспечить безопасную передачу информации по каналам связи с использованием технологии криптографической защиты информации. Защиту информации в сетях ISDN и IP предлагается обеспечивать с помощью аппаратуры «АТ-BRI» и криптомаршрутизаторов. Пример схемы организации видеоконференцсвязи представлены на рисунке 1.

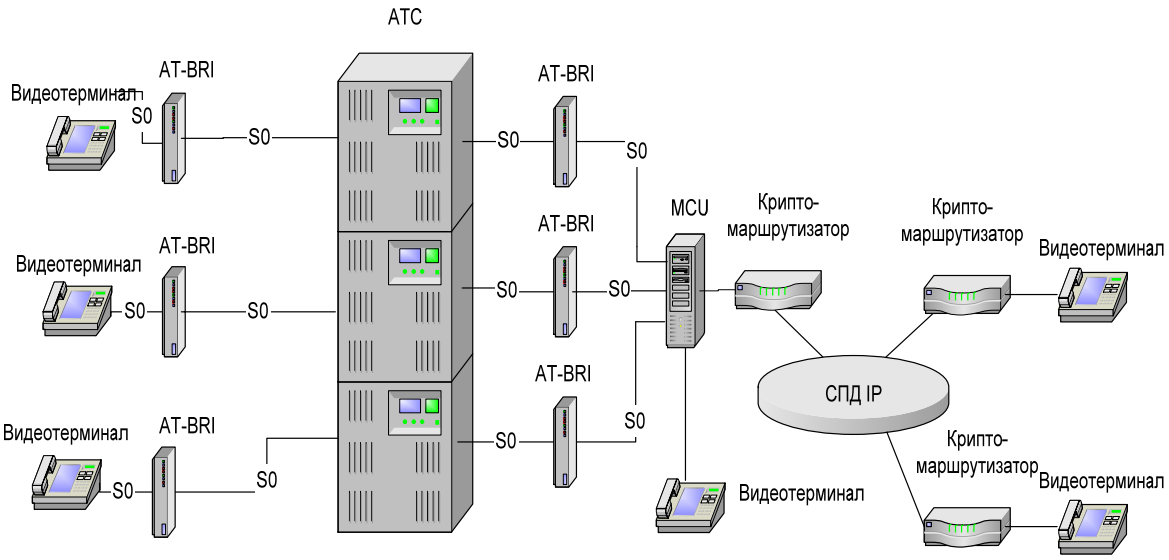


Рисунок 1

Абоненты могут подключаться к серверу управления многоточечными сеансами ВКС (MCU) через цифровую АТС или, по сети передачи данных IP. При этом скорость передачи информации по каналам ISDN будет составлять 128 кбит/с.

В случае применения у абонента сразу трех аппаратов «AT-BRI» или создания специального трехканального варианта – «AT-3BRI», возможно увеличение скорости передачи видео информации по каналам ISDN до 384 кбит/с.

Некоторые модели, например оборудование ВКС ViewStation MP, при соединении по ISDN позволяют проводить конференции с числом участников до 4 включительно без какого-либо дополнительного оборудования. Это обеспечивается наличием в каждом устройстве ВКС как минимум трех портов BRI.

Аппаратура «AT-3BRI» совместно с оборудованием ВКС ViewStation MP позволит организовать видеоконференцию с числом участников до 4 включительно без использования сервера MCU. Пример организации связи для этого случая представлен на рисунке 2.

Защита видеоконференцсвязи в сетях IP

В сетях IP хорошо зарекомендовали себя видеотерминалы ViewStation H.323. Видеотерминалы подключаются к сети IP по стыку Fast Ethernet (скорость работы 100Мбит\с).

Технологически построение защищенной IP-сети видеоконференцсвязи заключается в установке криптомаршрутизаторов (шифраторов IP-потоков) на выходах сегментов локальной сети.

Оборудование, использующееся в таких сетях видеоконференцсвязи, в частности, криптомаршрутизаторы, должно обеспечивать достаточную полосу пропускания и поддерживать режим QoS (Quality of Service).

Криптомаршрутизатор - специальное устройство, совмещающее в себе шифратор трафика, статический маршрутизатор и межсетевой экран. Каждый IP-пакет шифруется на индивидуальном ключе, что обеспечивает высокий уровень защищенности трафика.

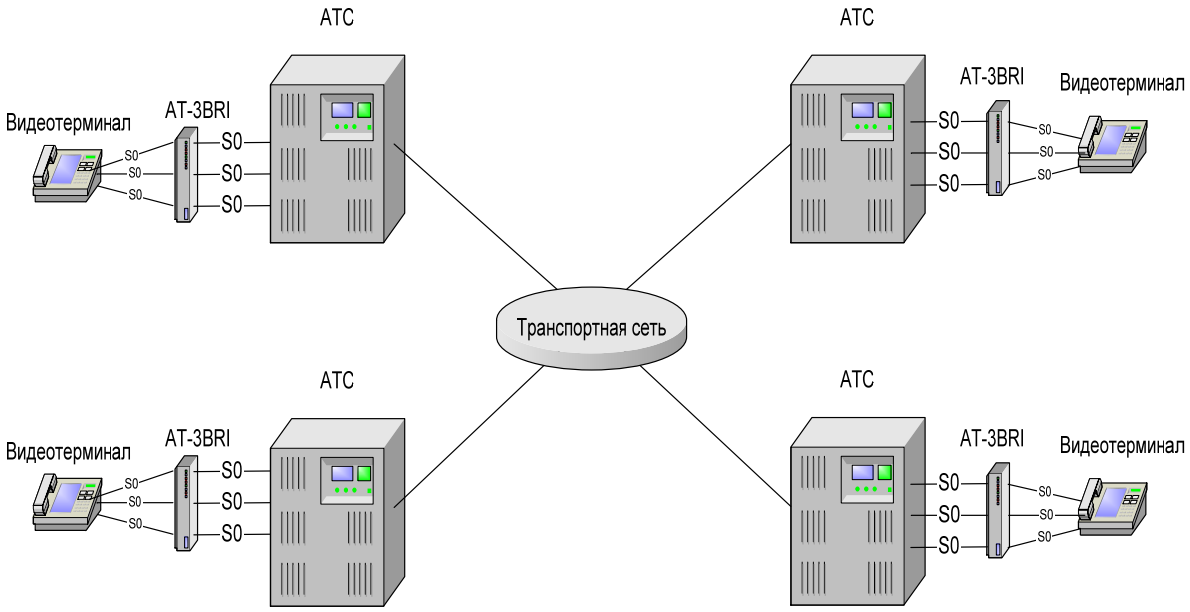


Рисунок 2

Криптомаршрутизаторы обеспечивают полную прозрачность для конечных пользователей, вместе с тем позволяют:

- скрыть структуру защищенной сети;
- защитить сеть от атак из вне;
- эффективно защитить передаваемую информацию;
- защитить потоки информации от анализа трафика;
- обеспечивать маштабируемость сети.

При работе криптомаршрутизаторы осуществляют преобразование трафика, при этом многие характеристики с точки зрения конечного пользователя меняются не лучшую сторону. Криптомаршрутизаторы вносят следующие изменения в работу сети:

- снижение пропускной способности сети
- увеличение накладных расходов на преобразование трафика;
- задержки при передаче пакетов.

Рассмотрим подробнее эти параметры.

Снижение пропускной способности сети возникает по разным причинам. Первая заключается в недостаточной производительности самих криптомаршрутизаторов, хотя, как правило, при выборе таких устройств этому параметру уделяется большое внимание. Криптомаршрутизаторы должны обладать достаточной пропускной способностью для того, чтобы минимизировать свое влияние при передаче информации в сети.

Вторая причина определяется типом трафика и обусловлена накладными расходами на преобразование трафика. Они возникают при обработке пакета за счет добавления нового IP-заголовка к туннелируемому пакету. Эта величина зависит от протокола, используемого в системе, и составляет фиксированное количество байт. Дополнительная нагрузка на сеть определяется процентным приростом длины пакета по отношению к исходной. В этом и заключается причина снижения пропускной способности в зависимости от типа трафика.

Например, широко известный протокол IPSec добавляет (для алгоритма ГОСТ 28147-89) при преобразовании минимум 54 байта. Для IP-пакета длиной

1500 байт (стандартный пакет передачи данных) прирост составит порядка 4%, а для 56 байтного пакета (IP-телефония) - накладные расходы составят уже около 100%.

Криптомаршрутизаторы вносят два типа задержек - прямую и косвенную. Первая обусловлена временем обработки пакета и зависит только от характеристик самого устройства. Вторая может возникать за счет увеличения трафика в канале из-за накладных расходов при туннелировании.

Для снижения задержек при передаче пакетов и поддержания высокого уровня качества обслуживания производительность криптомаршрутизатора должна быть примерно в два раза большей, чем скорость передачи информации в локальной сети, т.е. примерно 200 Мбит/с. Следует отметить, что достижение необходимой производительности весьма затруднительно, учитывая, что практически все отечественные криптомаршрутизаторы строятся на базе ПК. Решение указанной проблемы возможно во-первых путем разработки новой высокопроизводительной аппаратной платформы, во-вторых путем использования протоколов с минимальными накладными расходами на обеспечение конфиденциальности информации.

Во втором случае, следует отметить, что средства поддержки конфиденциальности, подразумевают, что весь трафик, между удаленными точками должен аутентифицироваться и шифроваться. Возможны два режима обеспечения конфиденциальности: туннельный и транспортный.

В туннельном режиме вся датаграмма IP, заголовок IP и данные передаются в зашифрованном виде. В транспортном режиме шифруются только данные, а заголовок IP передается в незашифрованном виде. Очевидно, что в туннельном режиме накладные расходы больше, чем в транспортом, так как после зашифрования к пакету добавляется новый IP-адрес. Это позволяет, скрыть структуру защищаемой сети путем анализа трафика, и тем самым предотвратить угрозу появления дальнейших атак. Однако, в корпоративных сетях сеть ВКС, чаще всего выделена в отдельную подсеть (например с помощью технологии MPLS), поэтому сокрытие информации о структуре данной сети не имеет практического смысла.

Кроме этого, необходимость применения технологии аутентификации трафика, при передаче между удаленными точками также недостаточно обоснована. Аутентификация трафика, позволяет обеспечить эффективную защиту от атак из вне. В этом случае любой принятый пакет не прошедший проверку аутентификации отбрасывается, тем самым, исключая попадание потенциально опасной информации в защищаемую сеть. В то же время, это не исключает возможность атаки на криптомаршрутизатор типа «Отказ в обслуживании» (denial of service — DoS). На проверку ложных и правильных пакетов тратится примерно одинаковое время, поэтому криптомаршрутизатор не обладающей достаточной производительностью может просто не успеть обрабатывать правильные пакеты, тратя все время на обработку и отбрасывание ложного трафика. Кроме этого, если сеть ВКС выделена с помощью технологии MPLS в отдельную подсеть, она не может быть связанна с внешними сетями, что значительно снижает вероятность злоумышленного проникновения в нее из вне. В связи с этим применение технологии аутентификации трафика при защите информации ВКС также избыточно.

Дальнейшее снижение накладных расходов вносимых криптомаршрутизатором, возможно с помощью применения решений основанных на использовании особенностей протокола передачи видеоинформации. Согласно рекомендациям H.323 видеоинформация передается с использованием протокола

RTP, обеспечивающего передачу данных в реальном времени. Использование особенностей данного протокола позволит обеспечить передачу шифрованной информации по сети IP, практически с нулевым уровнем накладных расходов.
Формат RTP-пакета в основном уже содержит все необходимые данные для надежной работы шифровального средства в условиях IP сети. Так например, поле «*Порядковый номер»* RTP-пакета может использовано для подгонки/осаживания шифратора в случае потери ряда пакетов, а поле «*Идентификатор источника синхронизации»* может быть использовано для формирования одинаковой синхропосылки шифраторов на приемной и передающей сторонах. Таким образом, в случаях где не требуется тунелирование и аутентификация трафика, для обеспечения конфиденциальности достаточно применить шифрование полезной нагрузки в RTP-пакетах, накладные расходы при этом будут отсутствовать. Аналогичный подход обеспечения конфиденциальности медиапотоков описан в рекомендации H.235, входящей в группу стандартов H.323. Потоки медиа информации шифруется криптоалгоритмом, после чего к ним добавляется заголовок протокола RTP. Поле «*Тип содержимого»* при этом может быть использовано для указания на номер используемого ключа шифрования.

В заключение хотелось бы отметить, что криптомаршрутизатор предназначенный для защиты сеансов ВКС, должен шифровать только медиа потоки и свободно передавать остальной трафик. В этом случае каналы не несущие конфиденциальной информации, такие как каналы управления оборудованием и сеансами ВКС будут передаваться в открытом виде. Это позволит снизить затраты на дополнительные криптомарщрутизаторы для рабочих мест администраторов и контроллеров зоны (привратников).
Если криптомаршрутизатор не обеспечивает функций привратника, то необходимо отметить, что защита ВКС, возможна, только когда привратник находится внутри защищаемой сети. Для организации защищенной ВКС в этом случае привратник должен быть выделен в отдельное устройство и устанавливаться внутрь защищаемой сети, что приводит к дополнительному увеличению стоимости решения.

Литература:

1. ITU-T Recommendation H.235 (2000), Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals.

Получено 16.11.2003. Доклад опубликован в Internet 24.11.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.78-80. Секция-8: Конфиденциальность, целостность, доступность.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/019)

БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ СЕТЕЙ СВЯЗИ И IP-ТЕЛЕФОНИЯ.

Разудалов П.Ю, Платонов А.А., Крупкин А.Ю.
Филиал ПНИЭИ - НИП "Аргус"

В настоящее время существует огромное число технологий и методов осуществления безопасности сетей корпоративных предприятий, поэтому безопасность является сложным и важным вопросом. Один из методов, предложенный ниже, можно рассматривать в качестве дополнения к комплексу стратегических решений в данной области, получивший свою актуальность в связи с широким распространением в настоящее время услуги IP-телефонии. Использование данной услуги привлекает возможностью осуществления "дешевых" междугородних внутрикорпоративных телефонных звонков.

Мероприятия, разрабатываемые в области безопасности должны проводиться на основе анализа рисков и возможных угроз. Существует несколько основных типов угроз, представляющих наибольшую опасность в сетях IP

- в момент передачи конфиденциальной информации о пользователях (идентификаторов, паролей) или конфиденциальных данных по незащищенным каналам, существует возможность **прослушивания** и **злоупотребления** ими в корыстных целях злоумышленником;

- возможность **манипулирования данными**, которые передаются по каналам связи;

- **подмена данных о пользователе** происходит в случае попытки выдачи одного пользователя сети за другого. При этом возникает вероятность несанкционированного доступа к важным функциям системы;

- **отказ в обслуживании** (denial of service -DoS) является одной из разновидностей атак нарушителей, в результате которой происходит вывод из строя некоторых узлов или всей сети. Она осуществляется путем переполнения системы ненужным трафиком, на обработку которого уходят все системные ресурсы. Для предотвращения данной угрозы необходимо использовать средство для распознавания подобных атак и ограничения их воздействия на сеть.

В настоящее время имеется достаточно широкий перечень средств, позволяющий бороться с выше указанными угрозами. Однако с помощью них не всегда возможно отследить и предупредить некоторые угрозы, вызванные даже непреднамеренными действиями некоторых пользователей IP-телефонии. Например, пользователь может настроить свой IP-телефон на использование кодека G.711, при передаче голосовой информации, которому требуется скорость 64 Кбит/с, для передачи голосового трафика чрез IP данному кодеку требуется уже около 96 Кбит/с. Учитывая, что скорость передачи информации в междугородних каналов передачи данных всегда ограничена, разговор такого пользователя может привести к отказу в облуживании других пользователей. Вероятность такого отказа тем более высока, так как трафик IP-телефонии, как правило, пользуется повышенным приоритетом при передаче.

С помощью специальной программы мониторинга (спуфинга), возможно отслеживание и прекращение деятельности таких пользователей.

Работа такой программы может быть основана на анализе поле “тип кодека” и длины пакетов. Типы кодеков и соответствующие им значения полей данных и длин пакетов, используемые в программах типа “NetMeeting” представлены в таблице.

Тип кодека	Значение поля “тип кодека” для речевого пакета	Длина пакета
U-Law 8кГц	0	276
G.723.1 8кГц 5333 бит/с	4	40
G.723.1 8кГц 6400 бит/с	4	44
A-Law 8кГц	8	276
CELP 8кГц 4,8кбит/с	96	32
SBC	96	Переменная
ADPCM 8кГц	96	276
G.711 A-Law 6.4к	8	180
G.711 U-Law 6.4k	0	180
G.711-ALaw-64k	8	260
G.711-uLaw-64k	0	260
GSM-06.10	3	152
G.729	18	80
LPC-10	7	48
G.726-32k	2	60
SpeexNarrow-18.2k	103	48
SpeexNarrow-15k	100	48
SpeexNarrow-11k	99	40
SpeexNarrow-8k	98	40
SpeexNarrow-5.95k	97	35

Примечание: значения полей и длин пакетов указаны в десятичной системе счисления.

Передаваемая по сети информация должна быть подвергнута анализу с целью выявления фаз начала установления соединений IP-телефонии по протоколам SIP и H.323, с последующим выявлением идентификаторов работающих пользователей и применяемых ими кодеков. В случае обнаружения пользователей нарушающих определенный для данной сети регламент, администратор безопасности должен принять меры по обеспечению нейтрализации такого пользователя.

Определение псевдонимов пользователей, участвующих в соединениях по H.323 протоколу, возможно в следующих случаях:

- перехват и анализ командных кадров (типа *Setup*, *Connect* и т.д.), которыми обмениваются пользователи непосредственно в момент установления соединения;

- перехват и анализ кадров RTCP, которые также содержат пользовательские идентификаторы.

Понятие «псевдоним пользователя» включает в себя разнообразную информацию: информация «Display» – в стандартных программах ip-телефонии (например, NetMeeting) эта информация выводится в окне «имя пользователя» (обычно содержит имя и фамилию пользователя, с которым установлено соединение); имя учётной записи пользователя; номер телефона; имя компьютера, которое используется для его идентификации в сети; имя пользователя, под которым он входит в систему, адрес его электронной почты и т.д.

При перехвате кадров *Setup* (или *Connect*) от обоих терминалов, считается, что новое соединение установлено. С этого момента все кадры, относящиеся к данному соединению, анализируются до тех пор, пока не будут перехвачены кадры от терминалов *Release Complete*. В этом случае считается, что текущее соединение разорвано.

Следует отметить, что в случае установление соединения по H.323 рекомендации предоставляется возможность максимально эффективной определения псевдонимы пользователей, участвующих в соединение.

Если для установления соединения используется SIP, то рассматриваются кадры *Invite*, *Ack*, *Bye*. При установлении соединения Источник в сторону Получателя отправляет кадр *Invite*. Данный кадр содержит имя учётной записи источника и получателя. При окончании соединения Источник в сторону Получателя посылает кадр *Bye*.

В случае установления соединения по SIP протоколу (с использованием proxy-сервера или без него) часто удаётся определить только имя учётной записи инициатора соединения.

Литература:

1. Иванова Т.И. Протокол H.323 в сетях IP-телефонии //ТСС, 2000, №2.

2. Уиллис Д. Что нужно для успешного внедрения IP-телефонии // Сети и системы связи, 1999, №4.

3. Иванова Т.И. Корпоративные сети связи. – М.: Эко-Трендз, 2001, 282 с.

Получено 20.11.2003. Доклад опубликован в Internet 2.12.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.81-86. Секция-8: Конфиденциальность, целостность, доступность.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/020)

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ С КОММУТАЦИЕЙ ПАКЕТОВ

Фунтиков Д.А.
Филиал ПНИЭИ - НИП "Аргус"

Введение

Развитие отечественных цифровых сетей в настоящее время происходит в основном за счет импортного оборудования. Потребности в современном оборудовании удовлетворяются такими крупнейшими зарубежными фирмами, как Alcatel (Франция), Siemens (Германия), Ericsson (Швеция), Philips (Голландия), Cisco Systems (США), Sony, NEC, Panasonic (Япония) и др. В то же время применение оборудования импортного производства повышает вероятность применения потенциальным противником различных видов разрушающих информационных воздействий и несанкционированного доступа к информации.

С целью повышение экономической независимости и информационной безопасности РФ необходимо в первую очередь поддерживать и развивать отечественный рынок телекоммуникационного оборудования. В целях обеспечение информационной безопасности государства, особое внимание, необходимо уделять производителям оборудования для магистральных сетей связи.

Следует отметить, что в настоящее время на рынке уже появились предложения оборудования для построения опорных оптоволоконных сетей выпускаемого несколькими отечественными компаниями. И хотя в этих устройствах используется преимущественно импортная элементная база, ряд компаний осуществляет их проектирование и изготовление в нашей стране. Данные изделия поддерживают не только традиционную архитектуру SDH и PDH, но и технологию уплотненного спектрального мультиплексирования (DWDM), получившую в последние годы широкое распространение

Как правило, опорная транспортную сеть является основой для построения целого ряда наложенных телекоммуникационных сетей различного назначения: цифровая телефонная сеть, интеллектуальная телефонная сеть, сеть передачи данных. При этом, предложения оборудования отечественного производства для построения вторичных сетей с коммутацией пакетов в настоящее время практически отсутствует. В этих условиях ключевым может стать вопрос выбора наиболее перспективной технологии пакетной коммутации. В настоящее время на эту роль могут претендовать технологии ATM, MPLS, IP и Frame Relay. Окончательный выбор, на наш взгляд, должен состояться с учетом устойчивости, той или иной технологии, к различным видам разрушающих информационных воздействий.

Вопросами обеспечения безопасности в подобных случаях достаточно давно занимаются многие зарубежные организации. Но, несмотря на это, положение дел в этой области еще далеко от совершенства. Наиболее давно изучаются вопросы безопасности IP-сетей. Результатом этой работы стал выпуск ряда рекомендаций под общим названием IPsec. В 1999г. ATM форум выпускает техническую спецификацию AF-SEC-0100.001 версии 1.0 посвященную вопросам

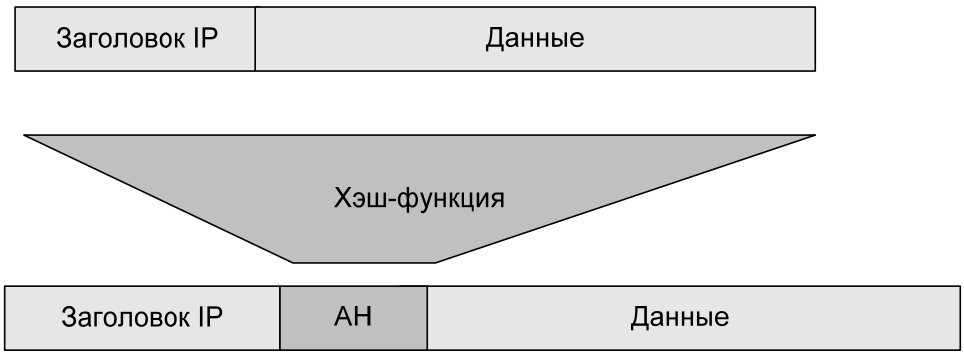
безопасности в ATM. В 2001г. выпущена версия 1.1 данной спецификации, в настоящее время работа в этом направлении продолжается. Вопросам безопасности в сетях Frame Relay посвящена спецификация FRF.17 выпущенная в 2000г. Технология MPLS в настоящее время не имеет достаточно проработанных механизмов обеспечения безопасности и не предусматривает защиту от атак изнутри.

Ниже приведен краткий обзор технологий безопасности применяемый в различных сетях с коммутацией пакетов.

Рекомендации безопасности IPsec

Проткол IPsec представляет собой набор стандартов, используемых для защиты данных и для аутентификации на уровне IP.

Для обеспечения требований аутентификации текущий стандарт предполагает применение хэш-функции, а точнее алгоритма не ниже MD5 с 128-разрядными ключами. Заголовок пакета и данные пропускаются через хэш-функцию, и результаты этого вычисления вводятся в специальное поле заголовка AH, как показано на рисунке 1.



Создание аутентификационного заголовка

Рисунок 1

Новый пакет с аутентификационным заголовком, расположенным между заголовком IP и данными, отправляется через маршрутизатор в пункт назначения. Проверка аутентичности производится путем вычисления хэш с помощью хэш-функции, далее сравнивается вычисленный хэш с параметрами, указанными в соответствующем поле AH. Если эти величины совпадают, аутентичность и целостность данных считается доказанной.

Средства поддержки конфиденциальности, подразумевают, что весь трафик, между удаленными точками должен аутентифицироваться и шифроваться. Возможны два режима обеспечения конфиденциальности: туннельный и транспортный.

В туннельном режиме вся датаграмма IP, заголовок IP и данные передаются в зашифрованном виде. В транспортном режиме шифруются только данные, а заголовок IP передается в незашифрованном виде.

Преимущества поддержки безопасности на сетевом уровне с помощью IPSec включают:

- поддержку совершенно немодифицированных конечных систем, хотя в этом случае шифрование нельзя назвать в полном смысле слова сквозным (end-to-end);
- частичную поддержку виртуальных частных сетей (VPN) в незащищенных сетях;
- поддержку транспортных протоколов, иных, чем TCP (например, UDP);
- защиту заголовков транспортного уровня от перехвата и, следовательно, более надежную защиту от анализа трафика;

- при использовании АН и средств обнаружения повторяющихся операций обеспечивается защита от атак типа «отказ от обслуживания», основанных на «затоплении» систем ненужной информацией.

Спецификация безопасности FRF.17

Спецификация FRF.17 определяет алгоритмы аутентификации, шифрования и обновления ключей. Аутентификация и шифрование могут использоваться независимо друг от друга, могут использоваться вместе или раздельно. Система обновления ключей может использоваться только вместе с шифрованием.

Следует отметить, что возможности аутентификации в спецификации FRF.17 ограничиваются средствами идентификации двух оконечных устройств и основываются на предварительно выбранном протоколе аутентификации (в рамках протокола PPP). Аутентификация происходит в момент установления связи, но может повторяться и после ее установления. Согласно данной спецификации средства аутентификации не являются обязательными.

Данная спецификация обеспечивает только конфиденциальность данных. Она не обеспечивает защиту от активных информационных атак. Эта спецификация определяет протокол, который обеспечивает некоторую защиту против пассивного подслушивания, и не защищает от активного нарушителя, который может подделать или изменять сообщения.

Как и в случае Ipsec, спецификация FRF.17 предусматривает добавление к пользовательским данным дополнительного заголовка.

Сеть Frame Relay действует на 2-ом уровне модели ВОС. В каждом кадре Frame Relay имеется заголовок, в котором располагается информация о принадлежности кадра к конкретному виртуальному соединению. Сеть Frame Relay использует только эту информацию, чтобы передать кадр через сеть. Это обеспечивает прозрачную передачу по сети зашифрованных кадров, без каких либо изменений в сети.

Спецификация безопасности ATM

Спецификация ATM AF-SEC-0100.001, определяет три сегмента — сегмент пользователя, сегмент контроля, и сегмент управления — каждый сегмент включает три или большее количество протокольных уровней — физический уровень, уровень ATM, Уровень Адаптации ATM (AAL), и верхние уровни при необходимости. Сегмент пользователя обеспечивает передачу данных пользователя через Виртуальные Подключения Канала и Виртуальные Подключения Пути. Сегмент контроля отвечает за установление соединения, разъединение, и другие функции связи. Сегмент управления выполняет функции управления и координирования, связанные, и с пользователем и сегментом контроля.

Данная спецификация определяет механизмы для аутентификации, конфиденциальности, целостности данных, и управления доступом для сегмента пользователя. Она также определяет механизмы аутентификации и целостности для сегмента контроля (сигнализации UNI и NNI). Защита сегмента управления исключена из этих технических требований; однако, так как объекты сегмента управления используют для своих целей соединения сегмента пользователя, защита сегмента пользователя может способствовать защите сегмента управления.

Таким образом, данная спецификация делает акцент на обеспечение защиты соединения, а не линии или узла.

Конфиденциальность сегмента Пользователя обеспечивает криптографические механизмы, которые защищают данные "пользователя" в виртуальном канале от неправомочного раскрытия.

Фиксированная длина ячейки ATM (53 байта) позволяет эффективно ее зашифровывать. Кроме того, только полезная нагрузка ячейки зашифровывается, заголовок передается в открытом виде. Это позволяет передавать зашифрованные ячейки через сеть без их расшифровки на промежуточных узлах.

Служба целостности данных в ATM обеспечивает механизм, который детектирует модификации значений данных или последовательности значений данных, даже в присутствии злонамеренных угроз модификации. Предусмотрены два режима защиты целостности: 1) целостность данных без защиты от переупорядочивания, и 2) целостность данных с защитой от переупорядочивания.

Когда целостность данных обеспечивается без защиты от переупорядочивания, источник добавляет в хвост каждого служебного модуля данных (SDU) криптографическую сигнатуру перед передачей. Эта сигнатура рассчитывается для всего SDU.

Когда целостность данных обеспечивает защиту от переупорядочивания "старый" или "переупорядочинный" SDU отвергается. Это достигается добавлением в хвост каждого SDU порядкового номера и затем вычисления сигнатуры на весь SDU, включая порядковый номер. Эта сигнатура, защищает и SDU и порядковый номер. Для надежного обеспечения целостности данных порядковый номер не должен повторяться в течение действия одного сеансового ключа. Схему обеспечения целостности в сети ATM иллюстрирует рисунок 2.

В ATM сеансовый ключ - это ключ, используемый непосредственно, для обеспечения конфиденциальности сегмента пользователя и служб целостности виртуального канала ATM.

Из-за потенциально высокой скорости передачи данных виртуального канала, необходимо периодически заменять эти ключи, чтобы избежать "перекрытия шифра". Технические требования ATM определяют службу обновления сеансового ключа, которая обеспечивает эту возможность.

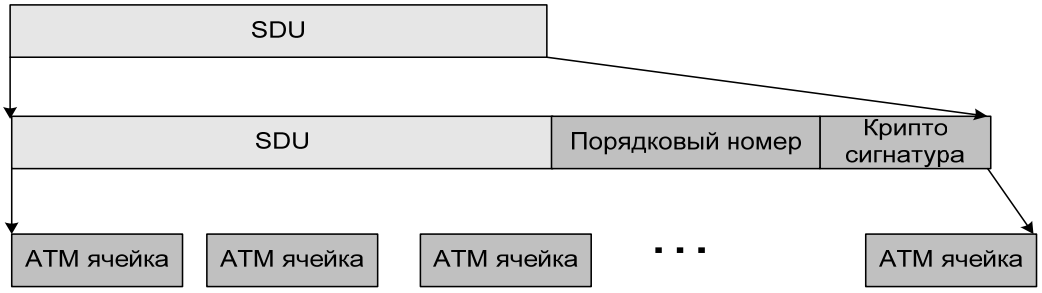
Эта служба состоит из двух этапов - этап обмена сеансовыми ключами и стадия замены сеансового ключа.

На этапе обмена сеансовыми ключами используется "мастер-ключ", который задается при начальной установке. Новый сеансовый ключ шифруется "мастер-ключом" и передается получателю. После получения зашифрованного сеансового ключа, получатель расшифровывает сеансовый ключ, используя, общий мастер-ключ, и хранит его до второй стадии - замены ключа.

Безопасность в технологии MPLS

Как отмечалось ранее, технология MPLS в настоящее время не имеет достаточно проработанных механизмов обеспечения безопасности и не предусматривает защиту от атак изнутри. Для повышения защищенности можно использовать протокол IPSec. Данный протокол может быть настроен на клиентском маршрутизаторе (CE) или может быть использовано специальное устройство. Использование данного протокола в первую очередь повышает безопасность информации пользователя, но не решает вопросы защиты маршрутизаторов от разрушающих информационных воздействий.

а) Обеспечение целосности без защиты от переупорядочивания



б) Обеспечение целосности с защитой от переупорядочивания

Рисунок 2

Сегодня технология MPLS получает все большее распространение, при организации виртуальных корпоративных сетей VPN. Основными достоинствами MPLS являются - повышение масштабируемости сети, обеспечение механизма качества обслуживания (quality of service - QoS) и управления трафиком (traffic engineering). Благодаря своим достоинствам, по мнению многих специалистов, MPLS в будущем вытеснит технологии ATM и Frame Relay из мультисервисных опорных сетей.

В сетях MPLS каждому IP-пакету присваивается специальная метка, определяющая его маршрут и приоритет. В результате технология MPLS может обеспечивать различные классы обслуживания (CoS), которые дают возможность использовать ее для транспорта различных видов трафика, в том числе мультимедийного.

Сеть MPLS включает в себя пограничные маршрутизаторы Label Edgle Router или Provider Edgle Router (PE) и опорные устройства сети MPLS – Label Switch Router или Provider Router (P).

Пограничные маршрутизаторы PE определяют какие услуги необходимы входящим IP-пакетам (например, предоставление QoS или управление полосой пропускания). В зависимости от этих требований, а также с учетом пункта назначения, PE маркирует IP-пакеты специальными метками. Таким образом, действия требующие больших вычислительных мощностей (анализ, классификация и фильтрация), выполняются только один раз, в точке хода.

Опорные маршрутизаторы P продвигают пакеты по сети только на основе меток и не анализируют заголовки IP-пакетов. В точке выхода из MPLS-сети метки удаляются.

В случае использования "чистой" сети на базе MPLS-VPN сервиса, где нет подключения к Интернету, защищенность такая же как и у протоколов ATM/FR. При подключении к сети Интернет, провайдер обязан "открыть" хотя бы один адрес PE маршрутизатора, что может повлечь за собой атаку.

Обычно в целях обеспечения безопасности провайдер и конечный пользователь не хотят, чтобы их сети были видны "снаружи", например из сети Интернет. "Невидимость" внутренних сетей является определенным барьером для потенциального злоумышленника. Если хотя бы один адрес из внутренней сети виден, то для злоумышленника нет сложностей провести атаку, например DoS. В идеале для сети MPLS видымыми адресами являются адреса CE и PE маршрутизаторов, а сама сеть не видна для атакующего.

Сложнее обстоит дело, если злоумышленник имеет возможность подключения, внутри самой сети. В этом случае не составляет труда провести атаку на любого подключенного пользователя, если только он не использует IPsec. Кроме этого возможно нападение на маршрутизаторы P и PE и изменение в них внутренних настроек и маршрутно-адресных таблиц. Последствия такой атаки могут, во-первых вывести сеть из строя, во-вторых привести к навязыванию ложных маршрутов, что в свою очередь может привести к утечке информации пользователей. Например, в результате атаки типа «человек в середине», при определенных условиях возможно вскрытие информации защищенной протоколом IPsec.

Защититься от внутренних атак на саму сеть возможно, только с помощью применения алгоритмов криптографической защиты управляющей информации, которой обмениваются маршрутизаторы CE, PE и P. Для защиты пользовательской информации необходимо применять тунелирование трафика на клиентском маршрутизаторе. Следует отметить, что применение протоколов безопасности собственной разработки, позволяет избавиться от многих недостатков IPSec, и снизить накладные расходы, увеличивающие длину пакета.

Заключение

Как видно из краткого обзора, приведенного выше, наиболее полно требованиям безопасности удовлетворяет протокол IPsec. В спецификациях ATM и Frame Relay основное внимание уделено обеспечению конфиденциальности информации. Защиту узлов и элементов сети от информационных атак данные спецификации не предусматривают.

Применение в сетях MPLS протоколов безопасности IPSec наряду с внедрением криптографических алгоритмов обеспечивающих защиту системы управления самой сетью позволит в будущем создавать опорные сети пакетной передачи данных полностью защищенные от информационного оружия, что в свою очередь позволит значительно укрепить информационную безопасность РФ.

Для быстрого достижения результатов в данном направлении необходима государственная поддержка. Компаниям, занимающимся вопросами безопасности, самостоятельное решение данных вопросов в настоящее время весьма затруднительно.

Литература

1. ATM Forum Technical Committee, «ATM Security Specification Version 1.1», af-sec-0100.002, March, 2001
2. FRF.17, D. Sinicrope (ed), Frame Relay Privacy Implementation Agreement, Frame Relay Forum Technical Committee, January 2000.
3. RFC 2401 (Security Architecture for the Internet Protocol).
4. RFC 2402 (IP Authentication header).

Получено 22.11.2003. Опубликовано в Internet 2.12.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.87-89. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/021)

УЧЕТ МАСШТАБА БИОМЕТРИЧЕСКОГО ОБРАЗА ПРИ ПРЕДСКАЗАНИИ КАЧЕСТВА ОБУЧЕНИЯ БИОМЕТРИЧЕСКИХ СИСТЕМ

Глухов Д.Н.
Лаборатория биометрических и нейросетевых технологий ПНИЭИ

Если сравнивать между собой биометрические технологии, способные обеспечить сохранение в тайне биометрического образа человека, то наиболее сильной оказывается технология, основанная на использовании рукописного почерка. Рукописный пароль проще всего сохранять в тайне. Голосовой пароль может быть перехвачен портативными записывающими устройствами. Клавиатурный почерк есть у очень малого числа людей и эта технология не может быть массовой. На данный момент можно считать, что наиболее сильной технологией, является идентификация человека по тайному рукописному образу. Очевидно, что качество этого типа систем существенно зависит от процедуры их обучения. Если систему обучать на достаточном числе стабильных образов, то она будет надежно работать правильно узнавая своего. Если образов мало и они нестабильны, то биометрические системы плохо учатся и плохо работают. Необходимо учитывать то, как система обучается.

На качество обучения биометрической системы влияет огромное число параметров. Граф, иллюстрирующий влияние различных параметров на качество биометрической системы, показан на рис. 1.

Рис. 1. Граф связей факторов и численных характеристик, учитываемых при синтезе прогнозов риска и ожидаемого уровня безопасности.

Возникает проблема определения качества принимаемых биометрической системой решений в зависимости от параметров биометрических образов, на которых она училась. Имеет смысл построить нейронную сеть, аппроксимирующую многомерную функцию зависимости качества биометрической системы от качества входных параметров.

Одной из основных проблем использования маленьких чувствительных экранов карманных компьютеров и ноутбуков является их низкая разрешающая способность. На рис. 2 приведены два примера введенных рукописных символов. Большое слово введено графическим планшетом малых размеров (чувствительная площадка 8x6 сантиметров). Маленькое слово введено через чувствительный экран карманного компьютера размером 4x5,5 сантиметров. Размеры полей этих устройств ввода сопоставимы, но все же появляется ощутимая разница масштабов образов. Последнее является следствием снижения разрешающей способности разнотипных устройств ввода графики и разной частоты их опроса.

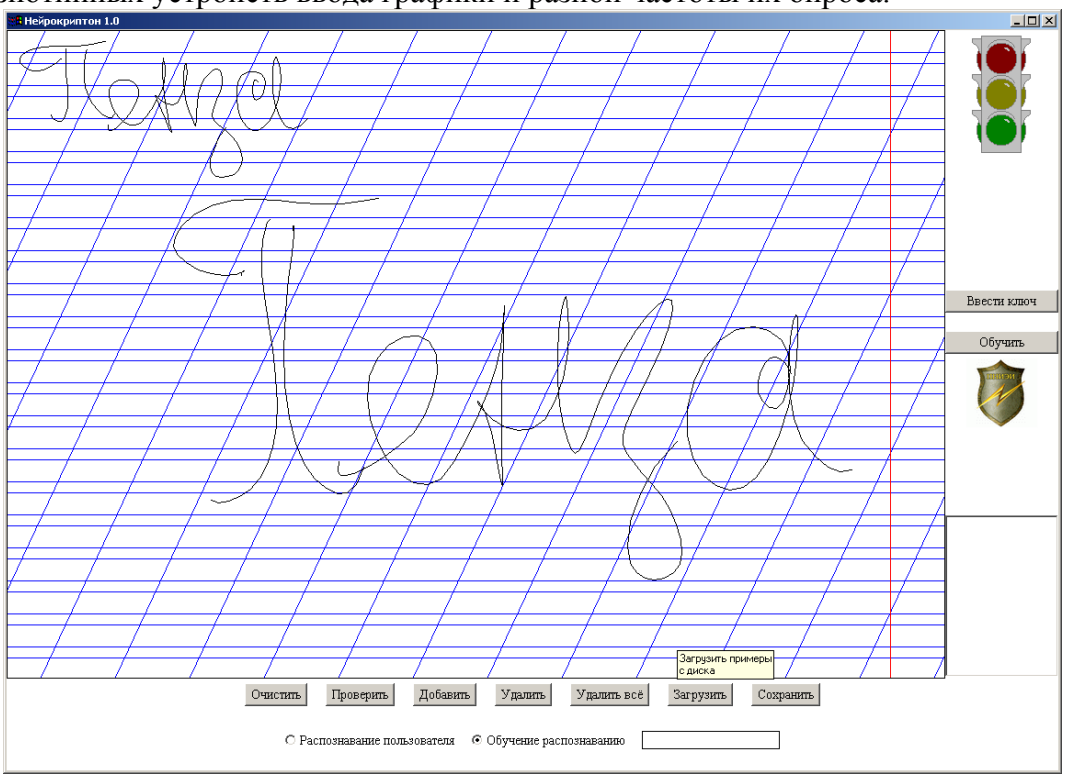


Рис. 2. Рукописное слово-пароль «Пенза», написанное с разным масштабом.

При написании рукописного слова-пароля в меньшем масштабе на графическом планшете (т. е. с достаточной частотой опроса координат пера) имеют значение только связи 3.10.1 и 3.10.3. Однако, при использовании сенсорного экрана карманного компьютера (рис. 3), все три связи 3.10.1-3.10.3 необходимо учитывать. Метрологические характеристики вводимой графики в карманные компьютеры существенно снижаются. В связи с этим необходимо в программном обеспечении предусмотреть учет влияния этих факторов на конечную надежность биометрической аутентификации [1,2].

Если строить универсальное программное обеспечение систем защиты на базе использования множества всех существующих средств ввода информации, то программа прогноза ожидаемого конечного качества защиты должна обязательно учитывать влияние погрешностей измерений положения кончика пера при вводе рукописного текста для разнотипных устройств ввода. На графе рисунка 1 эти связи имеют номера 3.10.1, 3.10.2 и 3.10.3 и далее связь 3.10.

Рис. 3. Использование карманного компьютера для ввода рукописной графики без специальных мер повышения частоты опроса сенсорного экрана.

Предварительные расчеты показывают, что некоторая потеря точности при использовании для ввода рукописной графики чувствительного экрана карманного компьютера не носит катастрофического характера. Конечные вероятностные характеристики системы биометрической защиты продолжают оставаться достаточно высокими, если принять меры по повышению частоты опроса чувствительного экрана и улучшению входной обработки данных за счет их сглаживания и промежуточной интерполяции. Задача создания универсальных программ биометрической защиты, способных работать со всеми видами устройств ввода графической информации реальна.

Синтез нейросетевого предсказателя качества принимаемых биометрической системой решений в зависимости от масштаба входных данных может быть осуществлен следующим образом. Путем статистических испытаний вычисляется качество для некоторого биометрического образа. Затем этот биометрический образ искусственно приводится к меньшему масштабу, и опять вычисляется качество. Вычислив, таким образом, значения функции качества в нескольких точках, можно построить нейросетевую аппроксимацию функционала связи масштаба входного образа и выходного качества.

В коммерческом продукте биометрического хранителя секретов необходим модуль, учитывающий все связи графа на рис. 1 и прогнозирующий качество биометрической системы для конкретного человека и для конкретного биометрического образа.

Литература:

1. Глухов Д.Н., Иванов А.И. Оценка стойкости биометрических образов человека. // Современные технологии безопасности, 2003, №2, с. 30-32.
2. Фунтиков В.А., Ефимов О.В., Иванов А.И. Биометрические технологии: автоматизированное прогнозирование уровня безопасности. //Защита информации. Конфидент. 2003. № 5, с.32-35.

Получено 24.11.2003. Опубликовано в Internet 4.12.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.90-92. Секция-3: Нормативное, методологическое, методическое обеспечение информационной безопаснисти.
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/022)

РАЗРАБОТКА МОДЕЛИ ПОЛЕЗНОГО СИГНАЛА ЧУВСТВИТЕЛЬНОГО ЭЛЕМЕНТА МАГНИТОМЕТРИЧЕСКОГО СРЕДСТВА ОБНАРУЖЕНИЯ

Захаров С.М. Дудкин В.А. E-mail: cirix@sura.net
Пензенский государственный университет

В настоящее время важной задачей в обеспечении контроля и управления доступом является обнаружение вооружённого нарушителя.

Эффективным способом решения этой задачи является использование магнитометрического способа обнаружения.

В качестве чувствительного элемента для магнитометрического средства обнаружения могут использоваться пассивные интегральные датчики магнитного поля, представляющие собой две прямоугольные катушки, подключенные дифференциально для компенсации синфазных помех. Принцип действия датчика основан на наведении ЭДС в пассивном контуре при проносе над ним ферромагнитной массы. Для использования современного подхода в проектировании подобных систем, необходимо создание математической модели полезного сигнала, снимаемого с чувствительного элемента.

Характеристикой, адекватно отражающей полезные магнитные свойства нарушителя на расстояниях, превышающих линейные размеры присущего ему намагниченного объема, является дипольный магнитный момент M, величина которого прямо коррелированна с массой ферромагнитного материала.

Математическая модель нарушителя представляет собой кусочно-гладкую ориентированную кривую Γ, моделирующую контур по которому течёт ток. Магнитный момент контура с током равен $M = I \cdot S$, где I - ток в контуре, S - площадь контура. При таком подходе в качестве модели нарушителя может быть использован круговой контур с током, геометрическое место точек которого определяется условием:

$$z = 0,$$
$$x^2 + y^2 = R^2,$$

где R - радиус контура с током.

Положительная нормаль к контуру с током выбирается параллельно оси z, порядок следования определяется по правилу левого винта.

При моделировании необходимо учитывать перемещение контура и его ориентацию контура в пространстве. Для задания ориентации контура в пространстве может быть использован поворот вокруг двух осей координат (оси y и вокруг оси z). Поворот осуществляется с помощью матриц линейного отображения:

Поворот вокруг оси y на угол $\alpha(t)$

$$x1 = x \cdot \cos(\alpha(t)) - z \cdot \sin(\alpha(t)),$$
$$y1 = y,$$
$$z1 = x \cdot \sin(\alpha(t)) - z \cdot \cos(\alpha(t)).$$

Поворот вокруг оси z на угол $\beta(t)$

$$x2 = x1 \cdot \cos(\beta(t)) - y1 \cdot \sin(\beta(t)),$$
$$y2 = x1 \cdot \sin(\beta(t)) - y1 \cdot \cos(\beta(t)),$$
$$z2 = z1.$$

С помощью данных матриц отображения можно задать зависимость ориентации контура во времени.

Задание движения достигается использованием матрицы линейного отображения:

$$x3 = x2 + x0 + v_x \cdot t + a_x \cdot t^2 + f_x(t),$$
$$y3 = y2 + y0 + v_y \cdot t + a_y \cdot t^2 + f_y(t),$$
$$z3 = z2 + z0 + v_z \cdot t + a_z \cdot t^2 + f_z(t),$$

где $x0, y0, z0$ - начальные координаты в момент времени *t=0;*

v_x, v_y, v_z - составляющие скорости движения контура с током;

a_x, a_y, a_z - составляющие ускорения;

$f_x(t), f_y(t), f_z(t)$ - функции, дополнительно определяющие параметры движения.

Поле контура в произвольной точке определяется следующим образом: вектор магнитной индукции. В в любой точке пространства определяется как сумма векторов *dB* создаваемых каждым элементом *dl* проводника с током. Элемент проводника *dl* создаёт поле с индукцией

$$\overrightarrow{dB} == \frac{\mu_0}{4\pi} \cdot \frac{I \cdot (\vec{dl}, \vec{r})}{r^3},$$

где $\frac{\mu_0}{4\pi} = 10^{-7}$ - константа; I – ток в контуре; $\vec{dl}$ - линейный элемент проводника с током (вектор, по направлению совпадающий с током);

$\vec{r}$ - вектор, соединяющий начало $\vec{dl}$ с точкой, в которой определяется магнитная индукция.

Если в качестве проводника с током задать круг, то можно получить источник магнитного поля с $M = I \cdot S$ Поле, создаваемое им, описывается выражением:

$$\vec{B} = \oint_{\Gamma} \frac{\mu_0}{4\pi} \cdot \frac{I \cdot (d\vec{l}, \vec{r})}{r^3} \cdot dl.$$

Чувствительный элемент представляет собой пассивный контур (использовано явление электромагнитной индукции) с определенными геометрическими размерами. Математически, чувствительный элемент представлен в виде двух направленных поверхностей $\overrightarrow{S1}$ и $\overrightarrow{S2}$.

$\overrightarrow{S1}$ удовлетворяет условию:

$$0 < x3 < l1,$$
$$0 < y3 < h1,$$
$$z3 = 0.$$

$\overrightarrow{S2}$ удовлетворяет условию:

$$l2 < x3 < 0,$$
$$0 < y3 < h2,$$
$$z3 = 0,$$

где *l1,l2* и *h1,h2* – длина и ширина первого и второго чувствительного элемента соответственно.

Положительная нормаль к поверхностям $\overrightarrow{S1}$ и $\overrightarrow{S2}$ сонаправлена с осью *z*.
ЭДС, возникающая в чувствительном элементе в магнитном поле *B* [1]:

$$\varepsilon = \varepsilon_1 - \varepsilon_2 = -\frac{d}{dt}\cdot \Phi 1 + \frac{d}{dt}\cdot \Phi 2 = -\frac{d}{dt}\int\limits_{\overrightarrow{S1}} \vec{B}\cdot d\vec{S}1 + \frac{d}{dt}\int\limits_{\overrightarrow{S2}} \vec{B}\cdot d\vec{S}2\,,$$

где *Ф1* и *Ф2* – поток вектора магнитной индукции;
S1 и *S2* –направленные поверхности.
Это выражение в скалярном виде выглядит следующим образом:

$$\varepsilon = \lim_{dS\to 0}\cdot(-\sum_{S1} B\cdot dS\cdot\cos(\alpha)) - \lim_{dS\to 0}\cdot(-\sum_{S2} B\cdot dS\cdot\cos(\alpha))\,,$$

где *dS*- элемент площади внутри, которого поле однородно (имеет одно направление и модуль);

α -угол между вектором $\vec{B}$ и нормалью к плоскости *dS*.

Если принять условие, что пассивный контур с током плоский, параллельный плоскости *X0Y*(в декартовой системы координат) и *dS*=*const*, то ЭДС в этом контуре равна:

$$\varepsilon_i = -\left|dS\right|\cdot(\frac{d}{dt}\cdot(\sum_{S1} B_z) - \frac{d}{dt}\cdot(\sum_{S2} B_z))\,.$$

Таким образом, задача нахождения напряжения в пассивном контуре сводится к нахождению проекции вектора *B*(источника поля с магнитным моментом *M*) на ось *z* в каждой точке плоскости, ограниченной контуром.

Уравнение для *z*-составляющей магнитной индукции в векторном виде представляет собой выражение[2]:

$$\overrightarrow{B_z} = \vec{k}\cdot\oint\limits_{\Gamma}\frac{\mu_0}{4\pi}\cdot\frac{I\cdot(x0\cdot y1 - y0\cdot x1)}{r^3}\cdot dl\,,$$

где $\vec{k}$ - единичный вектор параллельный оси *z*;
x0,y0,z0-координаты вектора *dl;*
x1,y1,z1-координаты вектора *r*.

Значения потока магнитной индукции записывается в массив данных. Производная по времени от потока находится как разность соседних значений потока, делённая на приращение времени. Предложенная математическая модель реализована в виде программы для ЭВМ. Расчёты с использованием предложенной модели позволили определить оптимальные параметры чувствительного элемента, исходя из максимального отношения сигнал/шум: (*h1=h2*=1.5м, *l1=l2*<500м). Установлено, что спектр мощности полезного сигнала лежит в диапазоне от 0 до 3.5 Гц, при скорости движения нарушителя до 5м/с, динамический диапазон полезного сигнала составляет порядка 40 Дб.

ЛИТЕРАТУРА:

1. И.В. Савельев «Курс обшей физики» том 2 М.1988 г.
2. Я.С. Бугров «Дифференциальные уравнения. Кратные интегралы. Ряды. Функции комплексного переменного.» М.1981 г.

Получено 10.12.2003. Опубликовано в Internet 14.12.2003.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 4. С.93-94. **СОДЕРЖАНИЕ**
Пенза-2003 (http://beda.stup.ac.ru/RV-conf/v04/023)

Труды научно-технической конференция
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Том 4.
Пенза -2003 г.

ЛР № 020779

Подписано к печати 22.03.2004 г.
Тираж 150 экз.
Усл. печ. л. 4,75.

Формат 60x84 1/16

Технический редактор А.Н.Шумаров
(841-2)63-81-15, 63-80-44

Издательство Пензенского научно-исследовательского
электротехнического института
440601, г. Пенза, ул. Советская, 9.

Отпечатано с готового оригинал-макета в информационно-издательском центре
Пензенского государственного университета. Заказ №
Бумага писчая № 1. Печать –RISO.
Пенза, Красная 40, т.: 52-47-33