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

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

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ТОМ 5

Пенза 2004

УДК: 681.322

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Труды научно-технической конференции под редакцией Волчихина В.И., Зефирова С.Л.. – Пенза – декабрь – 2004. Издательство Пензенского научно-исследовательского электротехнического института. Том 5. 108 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 5 содержит 23 статьи, отражающие точку зрения 40 специалистов по различным аспектам информационной безопасности.

ПОЧТОВЫЙ АДРЕС ОРГКОМИТЕТА: Россия 440017, 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/

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 5. С.3-7. Секция-2: Информационная безопасность сложных систем.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/001)

КАФЕДРЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ И ТЕХНОЛОГИЙ» ПЕНЗЕНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА – 50 ЛЕТ

Зефиров С.Л., Ольшевский Н.Н., Алексеев В.М., Кашаев Е.Д.
e-mail: ziss@beda.stup.ac.ru
Пензенский государственный университет

В 1953 г. специальным Постановлением Совета Министров СССР в Пензенском индустриальном институте была открыта специальность по подготовке разработчиков средств защиты информации для быстро развивающейся в те годы отрасли промышленности средств связи. В том же 1953 г. была основана кафедра «Электромеханическая аппаратура» (ныне «Информационная безопасность систем и технологий»). В течение более сорока лет (до 1996 г.) такие специалисты готовились только в г. Пензе на нашей кафедре.

За 50 лет для нужд отрасли подготовлено около 4000 специалистов, которые пополнили ряды инженеров-разработчиков, конструкторов, ученых, организаторов производства на предприятиях и организациях отрасли в Пензе, Москве, Санкт-Петербурге, Калуге, Львове, Новосибирске, Перми и других городах страны.

Среди выпускников кафедры – руководители и ведущие специалисты головных организаций отрасли, доктора и кандидаты наук, профессора, возглавляющие кафедры вузов Санкт-Петербурга, Волгограда, Пензы и других городов, лауреаты государственных премий, ответственные сотрудники государственных учреждений.

В течение двух последних десятилетий кафедра открыла свои филиалы на ведущих предприятиях города, разрабатывающих защищенные телекоммуникационные системы, системы управления, программные и аппаратные средства обеспечения информационной безопасности. Это такие предприятия, как ФГУП «Пензенский научно-исследовательский электротехнический институт», ГУП ПФ НТЦ «Атлас», ФГУП «НПП «Рубин», Научно-производственная фирма «Кристалл». На этих предприятиях ведется целевая подготовка студентов специальностей кафедры по индивидуальным учебным планам начиная с 4-го курса. Целевая подготовка позволяет сформировать специалистов, готовых к решению задач предприятия сразу после окончания университета. Специалисты предприятий, в свою очередь, привлекаются к учебному процессу на кафедре. Такое сотрудничество, выгодное и предприятиям, и университету, и кафедре, все более укрепляется. Выпускники, прошедшие индивидуальную форму подготовки, успешно продолжают работать на базовых предприятиях после окончания университета.

В настоящее время на кафедре работают 2 профессора, д.т.н. – Султанов Б.М., Расторгуев С.П., 14 доцентов, к.т.н. и к.ф.-м.н., в том числе член-корреспондент Академии криптографии РФ – Андрианов В.В.

Значительный вклад в совершенствование учебного процесса, подготовку научных и педагогических кадров и развитие материально-технической базы кафедры внесли в разные годы возглавлявшие кафедру доцент Астафичев Н.Д., к.т.н., доцент Поспелов Б.В., к.т.н., доцент Мартынов Ю.В., к.т.н., доцент Ольшевский Н.Н. и нынешний заведующий кафедрой – к.т.н., доцент

Зефиров С.Л. Высокий уровень педагогического и методического мастерства, научная эрудиция, внутренняя культура и культура общая – все это традиции кафедры, хранителями которых являются ветераны кафедры Андронов А.П., Алексеев В.М., Богданов В.В., Дорошкевич Л.Н., Иванов А.П., Кашаев Е.Д., Кузнецов Ю.А., Лукьянов В.С., Лупанов М.Ю., Миролевич В.Н., Никонов А.П., Султанов Б.В., Шутов С.Л. Большую поддержку в подготовке специалистов по защите информации, в развитии кафедры оказывает ректор Пензенского государственного университета, д.т.н., профессор Волчихин В.И. Благодаря решению ректора и с его помощью в 1998 г. на кафедре открыта еще одна специальность – «Комплексное обеспечение информационной безопасности автоматизированных систем».

Кафедра «Информационная безопасность систем и технологий» представляет Пензенский государственный университет в Учебно-методическом объединении по образованию в области информационной безопасности.

В настоящее время на кафедре готовят специалистов по защите информации по специальностям 075600 «Информационная безопасность телекоммуникационных систем» (специализация 075605 «Проектирование подсистем информационной безопасности телекоммуникационных систем») и 075500 «Комплексное обеспечение информационной безопасности автоматизированных систем» (специализация 075504 «Проектирование, мониторинг и аудит комплексных систем информационной безопасности»).

На кафедре открыта аспирантура по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность». Научными руководителями аспирантов являются к.т.н., доцент Зефиров С.Л.; д.т.н., профессор Чижухин Г.Н.; к.т.н., доцент Андрианов В.В. В университете с 1998 г. работает диссертационный совет по специальности 05.13.19, который возглавляет ректор университета, д.т.н., профессор Волчихин В.И. Преподаватели кафедры в совете защитили кандидатские диссертации на следующие темы: «Методы защиты программных средств вне доверенной вычислительной среды» (Цивин С.В.), «Методы и модели обеспечения информационной безопасности автоматизированных систем на физическом уровне» (Кашаев Е.Д.).

На кафедре к научно-исследовательской работе всегда привлекались и привлекаются талантливые студенты. Лучшие работы студентов ежегодно и небезуспешно представляются на университетские и всероссийские конкурсы студенческих работ. Из последних научных работ студентов отметим следующие. В 2001 г. на Всероссийском конкурсе студенческих работ (МТУСИ, г. Москва) студент Жуков С.В. за научную работу «Имитатор декаметрового канала» награжден дипломом Министерства образования РФ. В 2002 г. на Всероссийском конкурсе студентов по информационной безопасности «SIBINFO-2002» (Томский государственный университет систем управления и радиоэлектроники, г. Томск) доклад студента Лакина К.А. «Методы анализа данных аудита в системах обнаружения вторжений» признан лучшим. В 2003 г. на Всероссийском конкурсе студентов по информационной безопасности «SIBINFO-2003» доклад студента Спиридонова А.В. «Повышение производительности реализации схемы цифровой подписи за счет использования модуля специального вида» удостоен диплома III степени.

С первых лет существования кафедры научная деятельность ее коллектива связана с научно-исследовательскими и опытно-конструкторскими работами базовых предприятий и других предприятий ВПК. Научные исследования в 50–70-е годы прошлого века в рамках НИР развивались в следующих направлениях:

1. Исследование статистических характеристик служебных текстов (научный руководитель Астафичев Н.Д.).

2. Оптимизация защищенных печатающих устройств рулонных электронно-механических телеграфных аппаратов (научный руководитель Кузнецов Ю.А.).

3. Разработка комбинированного метода выделения основного тона речи (научный руководитель Поспелов Б.В.).

4. Разработка и изготовление параллельного формантного синтезатора речи с цифровым управлением для лингвистических исследований (научный руководитель Поспелов Б.В.).

5. Исследование процессов управления потоком и разработка концентраторов сообщений для сетей связи специального назначения (научный руководитель Лукьянов В.С.).

6. Разработка и исследование методов оптимизации комбинированных средств передачи для мобильных узлов связи (научный руководитель Мартынов Ю.В.).

Результаты НИР были внедрены в аппаратуру систем связи специального назначения.

В 80–90-е годы прошлого века успешно проведены НИР по следующим направлениям:

1. Разработка и исследование цифрового УПС для каналов ТЧ на скорость 9,6 кбит/с и 14,4 кбит/с (научный руководитель Ольшевский Н.Н.).

2. Исследование методов и средств измерения параметров и характеристик каналов связи (научный руководитель Богданов В.В.).

3. Исследование методов управления передачей информации в информационно-вычислительных сетях (научный руководитель Зефиров С.Л.).

В результате НИР по разработке и исследованию УПС для каналов ТЧ впервые в стране были созданы цифровые УПС на скорость 9,6 кбит/с и 14,4 кбит/с и внедрены в аппаратуру, находящуюся в настоящее время на вооружении Российской Армии. Проведенные в рамках НИР исследования адаптивных эхокомпенсаторов позволили реализовать двухпроводной дуплексный модем, по своим характеристикам превосходящий зарубежные аналоги.

Технические решения, полученные в результате НИР, защищены авторскими свидетельствами на изобретение и патентами:

– А.с. №1225034 Султанов Б.В., Афанасьев Л.Н., Шутов С.Л., Дорошкевич Л.Н., Райков В.Н. Цифровое устройство фазовой синхронизации;

– А.с. №1687010 Султанов Б.В., Афанасьев Л.Н., Шутов С.Л., Дорошкевич В.В., Климин В.П. Цифровой приемник дискретных сигналов;

– А.с. №1327307 Шутов С.Л., Султанов Б.В., Афанасьев Л.Н. Цифровое устройство фазовой синхронизации;

– А.с. №1510693 Афанасьев Л.Н., Дорошкевич В.В.., Райков Виктор Н., Райков Владимир Н., Султанов Б.В., Шутов С.Л. Приемник дискретных сигналов;

– А.с. №1693725 Султанов Б.В., Шутов С.Л., Афанасьев Л.Н., Дорошкевич В.В. Устройство восстановления несущего колебания сигнала данных;

– Патент на изобретение №2147791 Бочков В.К., Кирюхин М.С., Лысиков А.В., Миронов Н.П., Овчинкин Г.М., Оськин В.А., Прохоров А.Д., Султанов Б.В., Шутов С.Л. Дуплексный модем.

В результате НИР по исследованию методов и средств измерения параметров и характеристик каналов связи были разработаны: способ оперативного контроля состояния канала связи на основе измерения искажений контрольного сигнала специальной формы; устройства оценки состояния канала на основе измерения параметров «глазковой диаграммы»; регенератор цифрового

сигнала, устойчиво работавший при наличии в цифровом псевдослучайном сигнале специфических фрагментов, резко усложняющих возможности синхронизации аппаратуры связи. По результатам этой работы были получены следующие авторские свидетельства на изобретения:

– А.с. №1259497 Алексеев В.М., Ольшевский Н.Н. Способ контроля дискретного канала связи;

– А.с. №1241497 Алексеев В.М., Ольшевский Н.Н., Хижняк В.А., Хижняк О.А. Устройство для оценки состояния канала связи;

– А.с. №1434550 Хижняк В.А., Ольшевский Н.Н., Алексеев В.М., Броварник Д.С. Устройство для контроля состояния канала связи;

– А.с. № 1543562 Хижняк В.А., Алексеев В.М., Ольшевский Н.Н., Шутов С.Л. Регенератор цифровых сигналов;

– А.с. №991317 Алексеев В.М., Богданов В.В., Лачинов С.И., Султанов Б.В. Цифровой измеритель отношения двух напряжений;

– А.с. №1091182 Алексеев В.М., Богданов В.В., Султанов Б.В., Супонин Б.А. Устройство для перемножения напряжений.

В результате НИР по исследованию методов управления передачей информации были предложены методы управления обменом в сети связи и ряд устройств управления доступом абонентов в моноканал сети, реализующих различные методы доступа (случайный, детерминированный, со случайным порядком выхода, с учетом приоритета абонентов и сообщений). Ее результаты также защищались авторскими свидетельствами на изобретения:

– А.с. №1319040 Алексеев В.М., Зефиров С.Л., Пашанина А.А., Дорошкевич Л.Н. Устройство для сопряжения абонентов;

– А.с. №1336024 Алексеев В.М., Зефиров С.Л., Пашанина А.А., Богданов В.В. Устройство управления передачей информации в многопроцессорной системе;

– А.с. №1488822 Алексеев В.М., Голубев М.В., Зефиров С.Л., Чернова М.И. Устройство управления передачей информации в многопроцессорной системе;

– А.с. №1578827 Алексеев В.М., Зефиров С.Л., Лупанов М.Ю., Тумасов В.Д. Устройство для управления передачей данных по радиоканалу;

– А.с. №1614118 Алексеев В.М., Зефиров С.Л. Устройство управления передачей данных по радиоканалу.

Результаты научных исследований также публикуются в научных журналах «Электросвязь», «Радиотехника», «Вооружение» и сборниках научных трудов, обсуждаются на международных и российских НТК, излагаются в монографиях и научно-методических работах. Из последних научных работ преподавателей и сотрудников кафедры отметим следующие:

1. Алексеев В.М., Андрианов В.В., Зефиров С.Л. Международные критерии оценки безопасности информационных технологий и их применение: Учебное пособие. – Пенза: ПГУ, 2002.

2. Султанов Б.В., Щербаков М.А. Анализ цифровых систем фазовой синхронизации на основе функциональных разложений Вольтерра: Монография. – Пенза: ПГУ, 2002.

3. Султанов Б.В., Шутов С.Л., Захаренков В.Е. Измерения параметров эхо-сигналов в коммутируемых каналах передачи данных // Электросвязь. – 2002. – №10.

4. Зефиров С.Л. Управление информационной безопасностью живучих автоматизированных систем // Актуальные проблемы науки и образования: Труды Международного юбилейного симпозиума. Т. 2. – Пенза: Информационно-издательский центр, 2003.

5. Кашаев Е.Д., Егорова Н.А. Модель защиты сигналов на физическом уровне автоматизированных систем // Актуальные проблемы науки и образования: Труды Международного юбилейного симпозиума. Т. 2. – Пенза: Информационно-издательский центр, 2003.

6. Алексеев В.М. Состояние и проблемы нормативно-правового обеспечения информационной безопасности в российской федерации // Актуальные проблемы науки и образования: Труды Международного юбилейного симпозиума. Т. 2. – Пенза: Информационно-издательский центр, 2003.

На кафедре интенсивно внедряются новые информационные технологии в учебный процесс и в научные исследования. Этому способствует наличие компьютерных классов, постоянное подключение к *Internet*. С 1999 г. на сайте кафедры (*http://beda.stup.ac.ru/ziss*) непрерывно проводится научно-техническая интернет-конференция «Безопасность информационных технологий». Издано 4 тома тезисов докладов конференции.

В настоящее время сотрудниками кафедры ведутся научные исследования по следующим направлениям:

1. Обеспечение и аудит информационной безопасности организаций, информационных технологий и автоматизированных систем.
2. Разработка методов и моделей обеспечения информационной безопасности автоматизированных систем на нижних иерархических уровнях.
3. Исследование проблем преобразования сигналов в телекоммуникационных системах специального назначения.

Материалы поступили 01.02.2004. Опубликовано в Internet 20.04.2004

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.8-9. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/002)

ЭЛЕКТРОННЫЙ ПАСПОРТ ЗДОРОВЬЯ ГРАЖДАНИНА РОССИЙСКОЙ ФЕДЕРАЦИИ

Иванов А.И. E-mail:ivan@pniei.penza.ru; Кузнецов А.В.; Кисляев С.Е.
E-mail: k_s_e@mail.ru; Цунина Н.М.; Гелашвили П.А.
ПНИЭИ; Самарский государственный аэрокосмический университет; Самарский государственный медицинский университет

Все возможное многообразие криптографических протоколов и процедур разных служб и ведомств будущего информационного общества может быть сведено к одному единственному протоколу и процедуре, удостоверяющей конкретную личность в открытом информационном пространстве – электронному паспорту гражданина РФ. Одним из существенных элементов которого сертификат главного и единственного открытого ключа гражданина РФ со средствами удаленного криптографического биометрико-нейросетевого доказательства полномочий гражданина [1]. Один из информационных фрагментов будущего электронного паспорта гражданина РФ, видимо, должен относиться к состоянию здоровья гражданина. Введение подобной открытой информации в паспорт или введение ее в паспорт в зашифрованном виде оправдано. Быстрый доступ к закрытой и открытой достоверной медицинской информации о человеке (с его согласия и под его биометрическим управлением) в критических ситуациях может спасти ему жизнь. Какую часть информации открывать, а какую закрывать должен решать сам человек после консультации с врачом, однако такие данные как группа крови, острые аллергические реакции на лекарства, … Видимо, список неизменных биометрические параметров человека, открыто хранимых в его паспорте, должен сформироваться на основе практики.

Необходимость в хранении биометрико-медицинских данных в паспорте обусловлена тем, что вследствие сложившегося социально-гигиенического положения в России сохраняется тенденция к ухудшению здоровья населения. Интегральный показатель здоровья населения снижается, что приобретает характер нарастающей угрозы национальной безопасности (Потапов А.И., Ястребов Г.П., 1999 [2]). Дальнейшее развитие реформ в нашей стране, затронет и сферу медицинского страхования. Введение подобного документа оптимизирует управление медицинских служб, позволит более качественно анализировать информацию о состоянии здоровья населения, например, в любой части района города, что, несомненно, важно для решения задач социально-гигиенического мониторинга. Видимо, для открытого опубликования сведений о здоровье конкретного человека придется разрабатывать специальные индексы здоровья или иные интегральные показатели.

Несомненно, что подробная информация о состоянии здоровья гражданина РФ является конфиденциальной. Доступ к конфиденциальной информации паспорта должен иметь сам гражданин и лица, которым гражданин доверяет (постоянно или временно), несущие полную ответственность за сохранение конфиденциальности информации, к которой они получают доступ в ходе своей профессиональной деятельности. Более того, возможно создание механизмов не позволяющих копировать конфиденциальную информацию недобросовестным лицам (можно только увидеть, но сложно получить полноценную электронную копию).

Проблемы использования подробного конфиденциального электронного документа с конфиденциальной биометрией частично или полностью могут быть решены через создание специальных доверенных центров и разработку специальных криптографических механизмов защиты, опирающихся на использование главного личного ключа пользователя (личного ключа электронного паспорта).

Вопрос об элементах медицинского электронного документооборота открыт и требует обсуждения и разработки. Однако, по-нашему мнению, необходимо в электронном медицинском документообороте отражать результаты интегрального экспрессного изучения уровня здоровья и дееспособности людей с целью гигиенической донозологической диагностики, в том числе и для целей социально-гигиенического мониторинга. В связи с тем, что ряд показателей функционального состояния организма дифференцированно отражают воздействие экзогенных и эндогенных факторов. Использование функциональных проб рекомендуется рассматривать в комплексе с другими медицинскими критериями и учитывать, что большинство таких проб характеризует деятельность не одной отдельно взятой системы организма, а организма человека в целом (Цунина Н.М. и др., 2002 [3]).

Использование только одной функциональной пробы [4] для оценки кардиореспираторной системы подростков, в сочетании с определением вероятностных рисков здоровью, в качестве примера, позволил, оценить предотвращенный экономический ущерб от этих заболеваний, в 1999 и 2002 г. в г. Новокуйбышевске для 164 подростков в возрасте от 12 до 16 лет равный 180000 руб. (расчет на 2002 г.).

Введение подобных результатов функциональных проб, при профилактических осмотрах и диагностике заболеваний, сведение их и оценка, в виде например, величины территориального показателя адаптации популяции детей и подростков, и использование в электронном паспорте здоровья позволит направить усилия органов здравоохранения и других служб государства на благо гражданина РФ.

ЛИТЕРАТУРА:

1. Иванов А.И., Кисляев С.Е. Искусственные нейронные сети в биометрии, медицине и здравоохранении. *Монография*, Самара: ГП «Перспектива», 2004, 220 с.
2. Потапов А.И., Ястребов Г.П. Гигиенические аспекты в системе национальной безопасности/ Под общ. ред. акад. РАМН Потапова А.И. // Гигиенические проблемы охраны здоровья населения районов России в условиях реформирования системы здравоохранения: Сб. тез. Всерос. научн.-практич. конф. – М., 1999, с. 12–15.
3. Цунина Н.М. и др. Научные основы многоуровневой системы мероприятий по обеспечению гигиенической безопасности населения промышленного центра. *Монография*, Самара: ГП «Перспектива», 2002, 119 с.
4. Определение величины территориального показателя адаптации популяции детей и подростков в системе социально-гигиенического мониторинга. *Пособие для врачей*. / Под ред. академика РАМН, профессора А.И. Потапова. – Санкт-Петербург: СПбГМА им И.И. Мечникова; СамГМУ; ЦГСЭН в Самарской области, 2002. – 28 с.

Материалы поступили 12.02.2004. Опубликовано в Internet 20.04.2004

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.10-13. Секция-7: Аудит информационной безопасности.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/003)

ВЫДЕЛЕНИЕ ИНТЕРАКТИВНЫХ СЕССИЙ ПОЛЬЗОВАТЕЛЕЙ ПО ДАННЫМ ШТАТНОГО АУДИТА ОС HP–UX 11.x

Цукарев Э.В. E-mail: eddy@crystall.tl.ru
НПФ “Кристалл”

Недостатки подсистемы “аудит безопасности” в ОС

При разработке новых вычислительных машин и операционных систем к ним, ведущие мировые фирмы – производители, такие как Microsoft, Hewlett–Packard, IBM, Sun ставят в первую очередь задачи разработки высокопроизводительных, масштабируемых, безопасных вычислительных систем, которые удовлетворяли бы растущие запросы корпоративных заказчиков.

Современные UNIX–системы ведущих мировых производителей, а также ОС семейства Microsoft Windows NT/2K/XP имеют развитые средства обеспечения безопасности, что подтверждено сертификатами ведущих мировых институтов и организаций, занимающихся сертификацией информационных систем на соответствие стандартам безопасности.

Неотъемлемыми частями системной безопасности перечисленных выше ОС являются (см. документ [1]):

- идентификация пользователей;
- аутентификация пользователей;
- авторизация пользователей;
- аудит безопасности.

Аудит безопасности должен позволять однозначно соотнести операцию, выполненную пользователем (открытие файла, запуск программы и т. д.) с требуемой сессией пользователя на сервере/рабочей станции. На практике же, подсистемы аудита на всех выше перечисленных ОС являются “золушками”, реализация, которых оставляет желать лучшего. Желая скорее завершить этап разработки ОС и получить сертификат на соответствие “Common Criteria”, фирмы–производители зачастую формально подходят к реализации подсистемы “Аудит безопасности” в своих ОС.

Как пример можно привести реальный тестовый случай из отдела разработки информационных систем одной из компаний Пензы, специализирующейся на разработке корпоративного программного обеспечения. Пользователь **A** включил аудит на объекты на своей рабочей станции под управлением Windows XP и далее на директории “**test**” установил, что подвергаются аудиту все операции удаления файлов в данной директории и во всех нижестоящих относительно “**test**”. Каталог “**test**” должен быть разделяемым в сети “Microsoft Network” с правом изменения содержимого для всех пользователей. Пользователи **B** и **C**, каждый со своей рабочей станции, по локальной сети, по протоколу Microsoft Network совершают соединение на станцию пользователя **A**, совершив успешную аутентификацию с полномочиями пользователя “**Guest**”. Далее пользователь **B**, получив доступ к содержимому “**test**” удаляет один из файлов, расположенных в “**test**”.

Просмотрев “Security Log” штатного аудита Windows XP станции **A,** наблюдались следующие события:

- Вход пользователя “**Guest**” со станции **B**;
- Вход пользователя “**Guest**” со станции **C**;
- Удаление пользователем “**Guest**” файла в каталоге “**test**”.

Информации о том, с какой статнции произведено удаление файла, в “Security Log” не было. Это говорит о том, операция удаления файла не привязана к конкретной сессии пользователя.

Анализ штатного аудита ОС HP–UX 11.x, показывает, что в аудите есть информация о начале сессии пользователя в ОС, но чрезвычайно трудно визуально (анализируя текстовую распечатку аудита) определить какие именно операции выполнял пользователь, в течении сессии открытой на сервере/рабочей станции ОС HP–UX 11.x. Штатный лог содержит операции, выполненные всеми процессами в системе в том числе и системными сервисами, как правило, работающими от пользователя “**root**”. Все операции идентифицируются в штатном логе кодом, временем выполнения, кодом возврата и идентификатором процесса. В некоторых событиях штатного аудита, идентифицирующих операции присутствует идентификатор пользователя, но его наличие не говорит о том, что данную операцию выполнил пользователь, открывший интерактивную сессию на сервере/рабочей станции под управлением ОС HP–UX 11.x.

Операцию, которая отображается событием в штатном логе, мог выполнить один из сервисов ОС, штатное число которых насчитывает около сотни. Поэтому наличие идентификатора пользователя, равное нулю не говорит, о том, что операцию выполнил пользователь “**root**”, совершивший интерактивный вход на терминальную консоль сервера. Таким образом, визуально анализируя распечатку штатного лога аудита ОС HP–UX крайне трудно привязать операции выполненные, конкретными процессами к конкретному пользователю, имеющим открытые сессии на сервере/рабочей станции.

На основе вышеизложенного, можно сделать вывод, что остро встаёт проблема автоматизированной обработки аудита, снятого с серверов масштаба предприятия в корпоративной информационной системе. В специализированном центре сбора аудита, основу которого мог бы составить выделенный сервер, возможна реализация сбора аудита от нескольких серверов приложений UNIX.

Методика выделения пользовательских сессий

Визуальный анализ штатного аудита показывает, при удачной операции “**login**” порождается начальный процесс, идентификатор которого присутствует в аудите. Основная задача, которая стоит перед экспертной системой, функционирующей на сервере сбора аудита – построение дерева зависимых процессов. Причем каждое дерево будет иметь своё начало (корень) – от начального идентификатора процесса “**login**”. При поступлении события “**Вход пользователя в систему**” с флагом “**Успешный**” на анализ в экспертную систему, записывается **PID** данной операции как начало (корень) дерева.

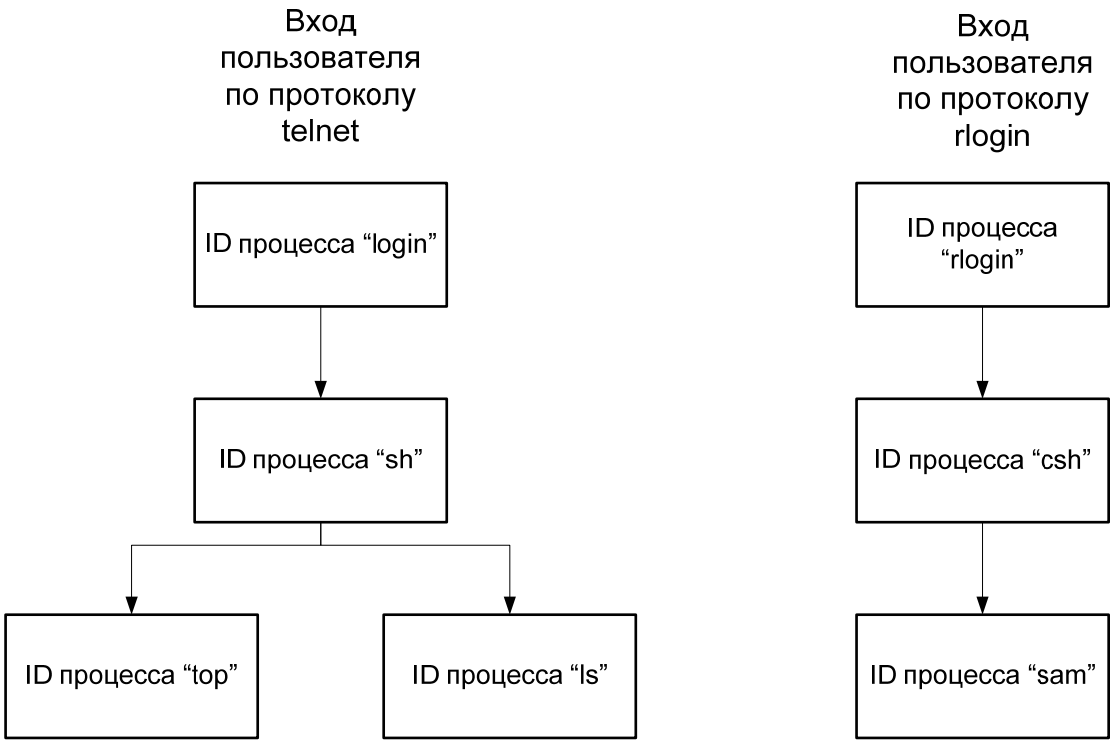


Рисунок 1 – Деревья пользовательских сессий

При поступлении событий “**fork**”, “**vfork**” (см. документ [2]) на вход экспертной системы производится следующий анализ: если родительские идентификаторы новых процессов входят в дерево (пользовательскую сессию) процессов, то и созданные процессы заносятся в одну из ветвей – ниже родительского процесса.

У событий – открытие файла, удаление файла, смена прав доступа и т. д. имеется поле – идентификатор процесса (**PID**), выполнивший данные операции. При поступлении данных событий на вход системы анализа поле **PID** проверяется на наличие в каждом дереве, если **PID** занесен в дерево процессов, то считается, данную операцию (открытие файла, смена прав доступа и т.д.) выполнил пользователь, открывший интерактивную сессию на сервере/рабочей станции ОС HP–UX 11.x. Если **PID** операции не был занесён в дерево процессов, то со всей уверенностью можно сказать операцию выполнил один из системных сервисов.

Удаление процессов из дерева производится при поступлении соответствующих событий “**exit**”, “**kill**”. При поступлении события завершения процесса “**login**” – удаляется всё дерево из памяти экспертной системы. Возможные примеры деревьев процессов – пользовательских сессий приведены на рисунке 1.

Возможно выделение пользовательских сессий открытых по следующим протоколам:

- telnet;
- rlogin;
- ftp;
- rexec.

Построение дерева процессов возможно при следующем минимальном наборе событий, включенном на регистрацию на сервере под управлением ОС HP–UX 11.x:

- Fork – порождение дочернего процесса;

– Vfork – порождение дочернего процесса;
– Execl – выполнение программы;
– Exit – завершение процесса;
– Kill – посылка сигнала процессу;
– Chdir – смена рабочего каталога.

При необходимости регистрации дополнительных операций пользователей, возможно включение на регистрацию в аудите дополнительных системных вызовов, которых насчитывается около 150 (см. документ [1]).

Доставка бинарных файлов аудита с серверов приложений в центр сбора аудита может осуществляться как организационными методами, так и с помощью специализированного программного обеспечения, которое устанавливается на сервер приложений и передаёт файлы аудита по запросу центра безопасности.

Специализированное программное обеспечение, инсталлируемое на сервер приложений ОС HP–UX 11.x , имеет возможность, опционально, собирать статистические параметры о всех запускаемых процессах в системе (объём занимаемой памяти, приоритет запуска и т. д.). Это позволит в центре безопасности дополнительно изучать параметры задач, запускаемых пользователями.

ЛИТЕРАТУРА:

1. Hewlett–Packard Comp. Administering a System: Managing System Security.
2. Hewlett–Packard Comp. HP–UX Reference Release 11.0. System Calls and File Formats.

Получено 31.05.04. Опубликовано в Internet 12.09.04.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.14-18. Секция-2 : Информационная безопасность сложных систем.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/004)

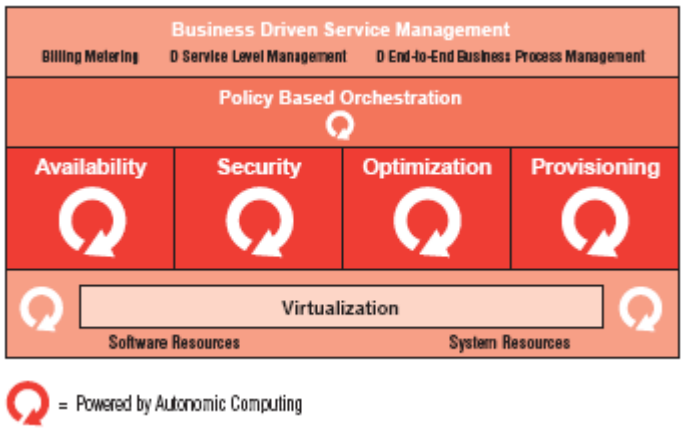
СОВРЕМЕННОЕ СОСТОЯНИЕ ДЕЛ В ОБЛАСТИ АДАПТИВНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Бочкарёв И.В. E-mail: igor@crystall.tl.ru
Научно-производственная фирма «Кристалл», г. Пенза

IT-индустрия последних 10 лет характеризуется постоянным увеличением сложности разрабатываемых компьютерных систем. В результате, всевозрастающая сложность систем сама становиться проблемой. С увеличением масштабов и изменением сетей и распределенных систем значительно увеличивается зависимость систем от стратегических ошибок разработки, ошибок в аппаратном и программном обеспечении, а также ошибок, связанных с человеческим вмешательством. Одновременно с этим возрастает роль и ответственность квалифицированного персонала в управлении систем. Все это в конечном итоге приводит к увеличению общей стоимости владения систем (TCO) и уменьшению коэффициента возврата инвестиций (ROI), фактически и определяющих реальные денежные затраты на обслуживание систем.

С целью решения данной проблемы компания IBM совместно с другими производителями выдвинули стратегию адаптивных вычислений (autonomic computing, AC), предназначенную именно для решения проблем сложности (complexity) систем за счет использования технологии нового поколения.

Образно, адаптивные системы можно представить как инфраструктуру, ориентированную на достижение некоторой цели, функционирующую в агрессивной быстро изменяющейся среде и не требующей вмешательства человека для определения и реализации оптимальной стратегии управления. В адаптивных системах выделяют несколько уровней: virtualization – уровень виртуализации программных и аппаратных ресурсов, services – сервисы, выполняющие функции самоадаптации (самовосстановление, самоконфигурирование, безопасность, самооптимизация), policy-based orchestration – политики управления, business-driven service management – уровень высокоуровневого управления системой. Каждый уровень представлен набором стандартных и унифицированных механизмов, протоколов и стандартов. Например, уровень виртуализации представляется через Grid – инфраструктуру виртуализации ресурсов, позволяющую объединить все программно-аппаратные ресурсы предприятия в один виртуальный компьютер, который способен перераспределять ресурсы по мере их необходимости. Использование Grid позволяет оптимизировать вычислительные ресурсы и данные, использовать их для всего рабочего процесса, разделять их по сети и обеспечивать их целостность. Уровень policy-based orchestration представляется совокупностью стандартизированных механизм



описания, представления, хранения знаний, представления и доставки высокоуровневых политик управления компонентами систем. Уровень сервисов представляется как набор адаптивных сервисов, имеющих стандартные интерфейсы взаимодействия, протоколы передачи, форматы данных, функционирующих на основании установленных политик.

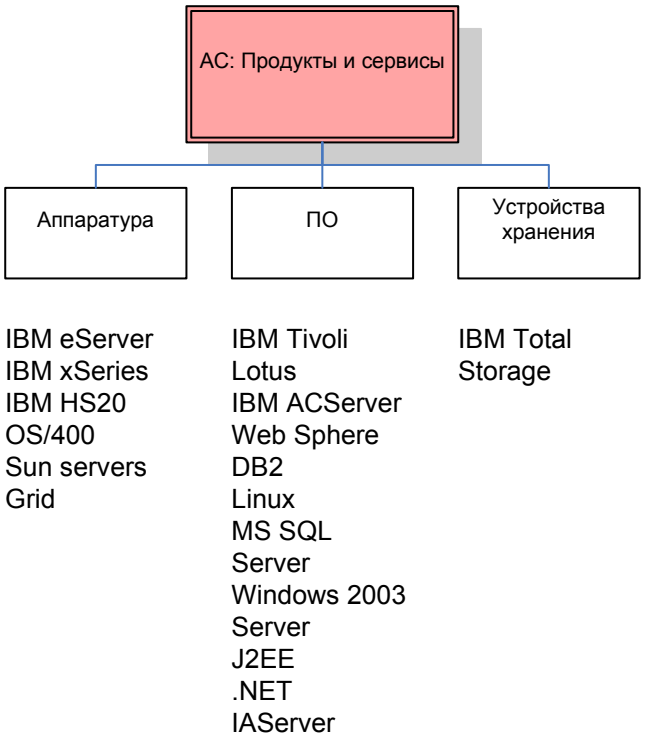
4 апреля 2003 года компания IBM совместно с рядом компаний анонсировании проект документа «An architectural blueprint for autonomic computing» («Проект архитектуры для автономных вычислений») [1], основное назначение которого обобщить знания в этой области и выработать общую архитектуру, а также ряд сопутствующих технологий и стандартов в сфере саморегулирующихся адаптивных систем. В рамках этого документа определены 4 концептуальные отправные точки адаптивных систем: самоконфигурирование, самовосстановление, самозащтита (безопасность) и самооптимизация. Кроме того, сформулированы и сгруппированы составляющие технологии для адаптивных систем: представление знаний, общее администрирование, комплексный анализ, политики управления и другие. В качестве практических механизмов реализации отдельных процедур функционирования или протоколов взаимодействия используются уже существующие и принятые стандарты де-факто: IETF, CIM, RFC, FIPA, Grid и многие другие. Другими словами, выполнена гармонизация документа с общепринятыми стандартами.

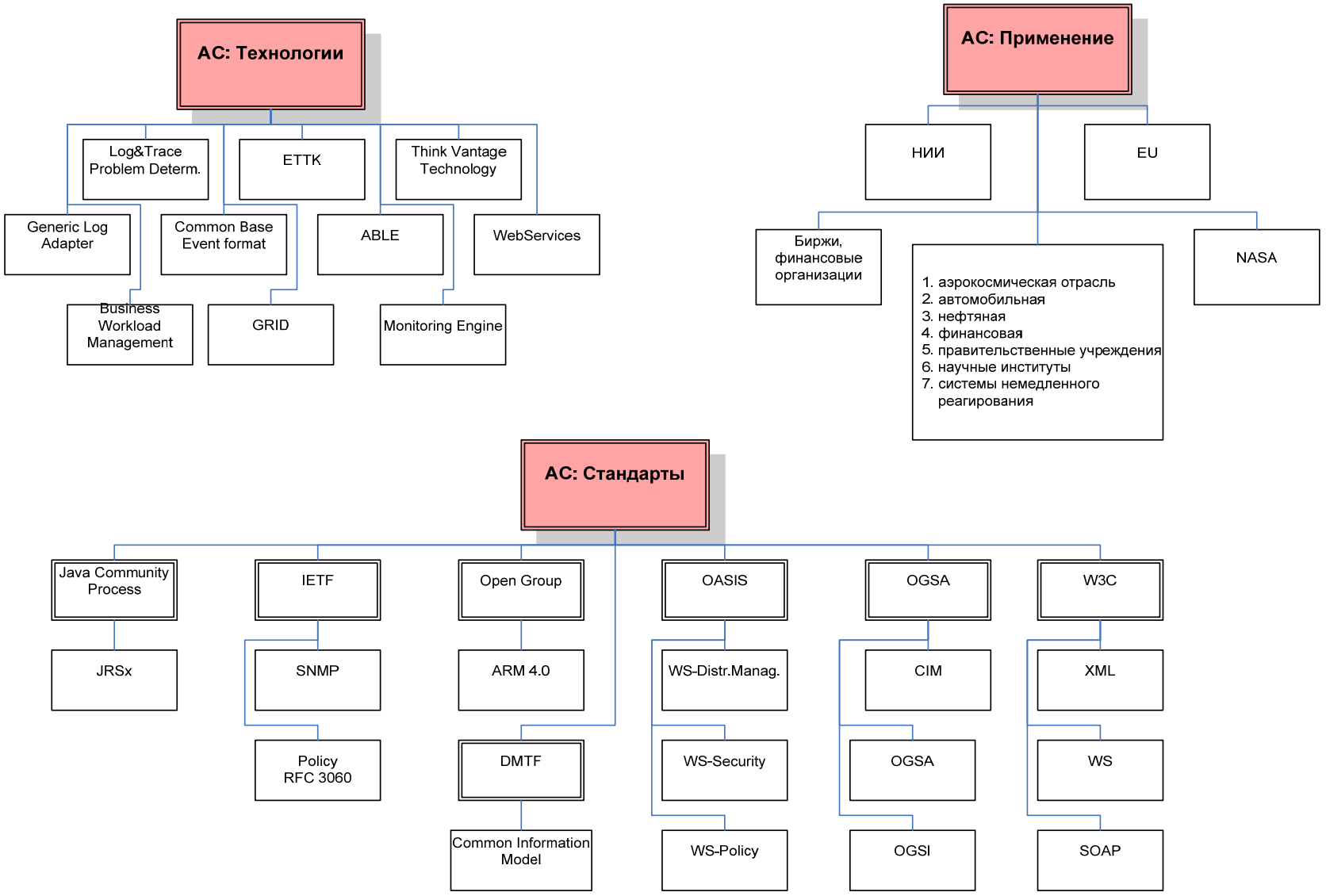
Цель данного документа, как заявляют представители IBM – разработать некоторый первоначальный вариант стандарта в области создания адаптивных систем, способных объединить все программные и аппаратные ресурсы различных производителей в рамках одной структуры предприятия, способной подстраиваться под изменяющиеся условия функционирования: сбои, ошибки, злоумышленных воздействия, нехватка ресурсов и т.д.

Уже через несколько месяцев, в октябре и декабре 2003 года IBM совместно с другими крупными производителями Cisco, HP, Sun выпускают ряд сопутствующих документов в области адаптивного управления и определения проблем (problem determination). Это «Adaptive Services Framework» («Инфраструктура адаптивных сервисов») [2] – IBM и Cisco, «Automated Problem Determination» («Автоматическое решение проблем») [3] – IBM совместно с Addamark Technologies, Opalis Software, Peregrine Systems, Singlestep Technologies, Vision Solutions. Кроме того, идет постоянная работа над развитием технологии Grid – «Open Grid Services Architecture» [4], являющейся базовой технологией для адаптивных систем. На сегодняшний день разрабатываются Grid 3-го поколения, также включающие большое количество технологий и стандартов управления распределенными вычислительными системами. Конечной целью этой инициативы является разработка стандартов в рамках организаций W3C, IETF (разработка RFC), IEEE, ISO.

Если говорить об общем количестве консорциумов и организаций, вовлеченных и развивающих данную тематику, то их насчитывается несколько десятков. Среди них: W3C (WWW Consortium), IETF (Internet Engineering Task Force), OASIS (Organization for Advancement of Structured Information Standards), FIPA (Foundation for Intellectual Physical Agents), SNIA (Storage Network Industry Association), GGF (Global Grid Forum), компании: IBM, Cisco, Sun, HP, Microsoft, Hitachi, Toshiba, Oracle, United Devices, BEA и многие другие. В рамках этих организаций уже разрабатывается и существует большое количество стандартов в области мониторинга распределенных систем, управления на основе политик и правил (OASIS, DMTF), виртуализации ресурсов (OGSA), представления данных (W3C), управления нагрузкой, администрирования, диагностики, установки решений и др.

Затрагивая практическую реализацию идеи адаптивных вычислений, можно сказать, что крупнейшие производители программного и аппаратного обеспечения уже сейчас предлагают широкий спектр решений. Так, например, IBM представлена на рынке как аппаратными и программными решениями: IBM eServer, xSeries, HS20, UsixServer, IAServer, OS/400, Tivoly, Lotus, WebSphere, DB2, Linux, Solaris и другие. Oracle, Microsoft ориентируют свои распределенные системы (SQL Server, Oracle 10g, Windows 2003 Server) на поддержку механизмов распределения нагрузки, унифицированного управления и прозрачной масштабируемости. Интересным является факт, что уже сейчас все продукты IBM, Cisco и ряда других компаний разрабатываются в соответствие с существующими стандартами в области адаптивных вычислительных систем и имеют множество механизмов интеграции (например, стандарт Common Base Event format [5] описывает правила представления любых событий аудита информационных систем). Cisco совместно с IBM предполагает разрабатывать расширенные Grid-сервисы для сетей хранения данных SAN. HP поддерживает соответствующие программные технологии на собственных аппаратных платформах (высокопроизводительных серверах, кластерах и системах хранения). Кроме того, HP предлагает собственную концепцию технологии Grid – UDC (Utility Data Center). Она подразумевает коммерческое использование Grid как технологии, которая обеспечивает минимальную нагрузку на средства передачи данных, решает проблемы защиты, распараллеливания баз данных и т.д. Технология управления распределенными ресурсами - важная составляющая и в стратегии N1 корпорации Sun Microsystems, направленной, прежде всего, на обеспечение управляемости информационной инфраструктуры в условиях возрастающей нагрузки и увеличения числа компонентов сети. Sun рассматривают технологии Grid как дополнение к существующему ряду продуктов корпорации - этот ряд включает мощные SMP-серверы с масштабируемой операционной системой Solaris, средства для построения вычислительных кластеров HPC Cluster Tools и пакет управления вычислительными ресурсами Solaris Resource Manager. Кстати, Sun эксплуатирует собственную Grid-сеть, объединяющую более 6000 процессоров и 210 Тбайт данных.




АС: Технологии
Log&Trace Problem Determ.
ETTK
Think Vantage Technology
Generic Log Adapter
Common Base Event format
ABLE
WebServices
Business Workload Management
GRID
Monitoring Engine
АС: Применение
НИИ
EU
Биржи, финансовые организации
1. аэрокосмическая отрасль
2. автомобильная
3. нефтяная
4. финансовая
5. правительственные учреждения
6. научные институты
7. системы немедленного реагирования
NASA
АС: Стандарты
Java Community Process
IETF
Open Group
OASIS
OGSA
W3C
JRSx
SNMP
ARM 4.0
WS-Distr.Manag.
CIM
XML
Policy RFC 3060
DMTF
WS-Security
OGSA
WS
Common Information Model
WS-Policy
OGSI
SOAP

Обобщая все вышесказанное, можно отметить, что концепция адаптивных вычислений является следующим шагом в эволюции компьютерных систем. Большинство критичных крупномасштабных систем требуют все больших затрат на сопровождение и управление все возрастающим парком программно-аппаратных ресурсов. Одновременно с этим, крах таких систем и последующее их восстановление, как правило, приводит потере времени и денег в размерах несопоставимых со стоимостью систем.

Концепция самостоятельного адаптивного управления систем на базе стандартных механизмов и протоколов позволяет развертывать системы, требующие минимального вмешательства со стороны персонала и способные функционировать даже в условиях внешних помех и злоумышленных воздействий.

Уже сейчас производители крупных вычислительных систем задумываются о необходимости стандартизации в этой области. На данный момент существует множество стандартов охватывающих различные аспекты функционирования адаптивных систем. Среди них: управление, представление знаний, управление ресурсами, безопасность и другие. На сегодняшний день данная область находится в начале своего развития, но с течением времени все большее количество производителей и международных организаций проявляет интерес к данной технологии с целью выработки общепринятых стандартов в области автономных вычислений.

ЛИТЕРАТУРА:

1. IBM and Autonomic Computing, An architectural blueprint for autonomic computing, Апрель, 2003. http://www-3.ibm.com/autonomic/pdfs/ACwpFinal.pdf
2. IBM and CISCO Systems. Adaptive Services Framework white paper, October 2003. http://www3.ibm.com/autonomic/library.shtml
3. IBM Autonomic Computing, Automating Problem Determination, October 2003. http://www-306.ibm.com/autonomic/r/pdfs/PD
4. Open Grid Services Architecture. http://www.globus.org/ogsa/
5. Specification: Common Base Event. http://www-106.ibm.com/developerworks/webservices/library/ws-cbe/

Получено 17.06.04. Опубликовано в Internet 12.09.04.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.19-24. Секция-3: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/005)

ПРОБЛЕМЫ NON-REPUDIATION

Спиридонов А.В. E-mail: spalex@crystall.tl.ru
НПФ «КРИСТАЛЛ»

Введение

Возможность успешного отказа пользователем от выполненных действий является серьёзной угрозой в системах с неполным доверием взаимодействующих сторон друг другу. Хотя на западе построением механизмов защиты от угрозы ложного отказа занимаются довольно продолжительное время и этому вопросу посвящены серьёзные работы и даже международные стандарты, в нашей стране до сих пор отсутствуют серьёзные публичные обсуждения non-repudiation. Тем не менее, с бурным ростом систем электронной коммерции данная проблема неумолимо приобретает всё больший вес. Уже накоплен печальный опыт инцидентов отказов, особенно в банковской сфере, показывающий, что решения проблемы наскоком, например, не до конца продуманным использованием цифровой подписи, не является приемлемым. Заинтересованные стороны вынуждены проявлять более интенсивный интерес к данной теме: делаются попытки осмысления и переработки западного опыта, регулирования и нормирования отношений с учётом обеспечения защиты от отказов.

Данная статья представляет частный взгляд на non-repudiation и даёт обзор некоторых проблем, связанных с ней.

Non-repudiation: как это по-русски?

В иностранной литературе и стандартах, посвященных информационной безопасности, non-repudiation стоит в одном ряду услуг защиты вместе с целостностью (integrity), конфиденциальностью (confidentiality), контролем доступа (access control) и аутентификацией (authenticity) [1]. В российском стандарте ГОСТ Р ИСО/МЭК 7498–2 [2], являющемся по сути переводом ISO 7498–2 [1], термин non-repudiation переводится как безотказность. Хотя такой перевод является практически дословным (non (англ.) – не; repudiation (англ.) – отказ), трудно назвать его удачным, поскольку термин «безотказность» в России уже имеет достаточно устоявшийся технический характер и используется при обсуждении надежностных качеств тех или иных изделий, систем и т.д. Применение его для обозначения услуги защиты видится не совсем приемлемым, потенциально ведущим к путанице. Варианты «бесспорность» и «неоспоримость» не совсем отражают сущность non-repudiation, основное предназначение которой всё же в защите от отказа, а не от спора в общем случае, но об этом речь пойдёт ниже. Поэтому в данной статье в качестве русскоязычного аналога термина non-repudiation используется похожий, но более нейтральный, по мнению автора, термин – неотказуемость.

Назначение и определение

Что подразумевается под неотказуемостью? В литературе встречаются различные определения неотказуемости, зачастую не совсем похожие друг на друга.

Например, согласно [3] неотказуемость – это категория защиты, обеспечивающая возможность верификации источника конкретного сообщения третьей стороной.

Согласно же [4] неотказуемость есть услуга безопасности, обеспечивающая невозможность отказа со стороны субъектов, задействованных во взаимодействии, от выполненных ими действий.

В стандарте ISO/IEC 13888 [5], посвященном вопросам обеспечения неотказуемости, сказано, что целью услуги неотказуемости является генерация, сбор, хранение, предоставление и проверка свидетельств относительно заявленного события или действия, а также предоставления механизма разрешения споров о существовании или несуществовании данного события или действия.

Несмотря на некоторые различия в определениях, можно выделить следующие ключевые моменты относительно неотказуемости, присутствующие в том или ином качестве у всех авторов:

– основным назначением неотказуемости является обеспечение такого режима взаимодействия заинтересованных сторон, при котором ни одна из сторон не может успешно отказаться от заявленных ею реально совершенных действий или имевших место событий;

– в рамках обеспечения неотказуемости должны генерироваться, собираться, сохраняться и предоставляться неопровержимые проверяемые тем или иным способом доказательства заявленных событий и действий – свидетельства неотказуемости. Такие свидетельства должны позволять однозначно разрешать споры по поводу существования или несуществования заявленного события или выполнения или невыполнения той или иной стороной заявленного действия;

– свидетельства неотказуемости должны иметь силу с точки зрения третьей стороны, привлекаемой для разбора конфликта между двумя сторонами.

Главным признаком необходимости привлечения механизмов неотказуемости для защиты взаимодействия некоторых сторон является априорное недоверие этих сторон друг другу, подразумевающее существенную вероятность отказа одной из сторон от реально выполненных ею действий или оспаривания реально имевших место событий. В системах, в которых стороны доверяют друг другу либо отказ не может принести выгоды отказывающейся стороне, в том числе косвенной выгоды, или убытка другой стороне, речь о неотказуемости не идёт, поскольку её обеспечение является необоснованным.

Место среди других услуг защиты и суть non-repudiation

Все услуги защиты тесно взаимосвязаны. Тем не менее, каждая из них достигает вполне конкретных целей.

Аутентификация обеспечивает защиту от атаки типа «маскарад» – выступления от имени легального субъекта кого бы то ни было, не уполномоченного на это. Как правило, уполномоченным является только сам субъект. Аутентификация данных защищает аналогичным образом данные, т.е. позволяет некоторым субъектам проверять тот факт, что данные созданы заявленным субъектом. Аутентификация данных подразумевает контроль их целостности.

Контроль доступа обеспечивает защиту от неавторизованного доступа к защищаемым ресурсам.

Конфиденциальность обеспечивает защиту от неавторизованного ознакомления с информацией.

Целостность данных обеспечивает их защиту от неавторизованного создания, изменения и уничтожения.

Неотказуемость должна защищать от ложного отрицания существования или несуществования того или иного события или выполнения или невыполнения того или иного действия.

Каждая из услуг защиты предоставляет некоторые свидетельства обеспечиваемых ею свойств безопасности. Например, свидетельства целостности, посредством проверки которых осуществляется контроль целостности данных, свидетельства аутентификации, по результатам проверки которых принимается решение об авторизации заявленных субъектов или подлинности предоставленных данных и т.д. Также и неотказуемость предоставляет некоторые свидетельства неотказуемости, которые позволяют разрешать конфликты, вызванные оспариванием одной из сторон того или иного действия или события.

Основной вопрос данной статьи: какова необходимость в выделении неотказуемости как отдельной услуги при гарантированном предоставлении остальных четырёх услуг защиты? Нужны ли дополнительные механизмы неотказуемости, если в системе уже надежно обеспечены аутентификация, контроль доступа, целостность и конфиденциальность? Чтобы попытаться ответить, следует рассмотреть возможные конфликты неотказуемости.

Для простоты будем рассматривать обеспечение неотказуемости при обмене некоторыми сообщениями между двумя сторонами – этот случай несложно развить до общего случая отказа от действия или отрицания события. Предположим, что в системе используются протоколы передачи сообщений с подтверждением доставки – действительно, если отправитель не знает, получил ли получатель сообщение, то какой смысл это оспаривать? Также предположим, что в системе надёжно реализованы базовые услуги защиты: аутентификация субъектов и сообщений, контроль целостности сообщений и контроль доступа (обеспечение конфиденциальности с точки зрения неотказуемости не играет важной роли).

Для случая передачи сообщения от стороны *A* стороне *B* можно выделить два типа конфликтов неотказуемости:

a) сторона *A* заявляет, что получила сообщение от стороны *B*, которая в свою очередь заявляет, что не отправляла данного сообщения стороне *A*;

b) сторона *A* заявляет, что отправляла сообщение стороне *B*, которая в свою очередь заявляет, что не получала его.

На самом деле, конфликт типа b) можно свести к конфликту типа a), поскольку он есть конфликт типа a) относительно подтверждения получения сообщения со стороны *B* (очевидно, что для аутентификации такого подтверждение должны применяться средства не менее строгие, чем для аутентификации самого сообщения). Далее рассматривается только конфликт типа a).

При конфликте возможны четыре варианта реального поведения сторон и соответственно четыре результата его расследования:

- сторона *A* лжёт, сторона *B* утверждает истину;
- наоборот: сторона *A* утверждает истину, сторона *B* – лжёт;
- обе стороны утверждают истину;
- обе стороны лгут.

Последний вариант маловероятен, поскольку трудно представить подобную ситуацию, при которой обеим сторонам выгодно лгать. Скорее всего, такие действия будут связаны со сговором сторон с целью обмана некоторой третьей стороны, что ведёт к выходу конфликта за рамки взаимодействия двух

сторон и требует дополнительного более широкого рассмотрения. Хотя совсем исключить случай, когда обе стороны лгут, нельзя, однако подобный вывод сделать в результате расследования конфликта между ними практически невозможно.

Третий вариант возможен только при вмешательстве некоторого внешнего злоумышленника путем реализации атаки типа «третий посередине», которая в свою очередь базируется на атаке типа «маскарад». Это означает ненадёжность используемых механизмов аутентификации, что противоречит начальным предположениям о системе.

Первый и второй варианты поведения, при которых одна из сторон лжет, а вторая заявляет истину, допустимы и равновероятны, и именно они в ходе расследования конфликта неотказуемости рассматриваются как основные.

Возможны два истинных положения вещей при конфликте:

– сообщение действительно передавалось. Тогда сторона *A* говорит истину, а сторона *B* лжёт;

– сообщение не передавалось. Тогда сторона *A* лжёт, а сторона *B* говорит истину.

Чтобы провести мошенничество стороне *A* необходимо подделать свидетельство аутентификации стороны *B*, поскольку только на основании получения такого свидетельства *A* могла принять спорное сообщение за подлинное.

Здесь ключевым моментом становится свойства, обеспечиваемые аутентификацией. Как было сказано выше, аутентификация подразумевает защиту от атаки типа «маскарад». Вопрос в том, является ли «маскарадом» в данном случае действия стороны *A*? Если это «маскарад», а судя по определению «маскарада» это действительно так, тогда защищать от подобной подделки свидетельств аутентификации должны сами механизмы услуги аутентификации. При априорной надёжности этих механизмов подделка свидетельств аутентификации невозможна. В этом случае конфликт типа а) разрешается проверкой представленного стороной *A* свидетельства аутентификации спорного сообщения – положительный результат проверки говорит о правоте стороны *A*, отрицательный – о правоте стороны *B*. Потребности в дополнительных механизмах защиты и расследования не возникает.

К сожалению ситуация всё-таки сложнее, поскольку на практике аутентификация обычно используется только в контексте защиты в реальном времени. В простейшем случае отправитель и получатель обладают некоторым общим секретом. С использованием этого секрета отправитель вычисляет свидетельство аутентификации сообщения для каждого отправляемого получателю сообщения. Получатель проверяет корректность полученного с сообщением свидетельства. Так как он уверен в том, что это не он создал сообщение и свидетельство и что секретный ключ кроме него самого известен только отправителю, в случае успешной проверки свидетельства он аутентифицирует полученное сообщение. Однако никому кроме себя доказать тот факт, что не он сам изготовил это свидетельство, получатель не может, поскольку механизм аутентификации позволяет ему это сделать.

Для решения данной проблемы и вводится услуга неотказуемости. Но причина проблемы в использовании недостаточно надёжных механизмов аутентификации. Т.е., по сути, обеспечение неотказуемости сводится к формированию более сильных свидетельств аутентификации, а сама неотказуемость есть крайняя форма аутентификации. Действительно, если используется аутентификация, предотвращающая «маскарад» полностью, то о неотказуемости речи не идёт, поскольку в системе невозможно подделать

сообщение. Так почему же неотказуемость всё же выделена в отдельную услугу защиты?

Видятся две основные причины. Во-первых, как было сказано выше, в сложившейся криптографической практике термин «аутентификация» используется обычно для обозначения защиты от атаки типа «маскарад» только со стороны внешнего злоумышленника. Так сложилось исторически и для многих систем безопасности такого понимания аутентификации вполне достаточно – добавление в аутентификацию свойств защиты от отказа делает этот термин не совсем однозначным. Во-вторых, преследуемые неотказуемостью цели играют очень важную роль в современном бизнесе, являющемся основным потребителем систем обеспечения информационной безопасности. Вопросы обеспечения неотказуемости чрезвычайно важны во многих областях бизнеса, особенно в электронной коммерции. Свидетельства неотказуемости становятся важным гарантом честности проводимых сделок, аргументом, используемым при разрешении конфликтов вплоть до использования в судах. Всё это позволяет рассматривать неотказуемость как обособленную услугу защиты.

Заключение

В связи с бурным ростом электронных способов ведения бизнеса неотказуемость начинает играть всё большую и большую роль в обеспечении информационной безопасности. Зачастую от успешного обеспечения неотказуемости напрямую зависит успех коммерческого предприятия, бизнеса. На западе проблемы обеспечения неотказуемость обсуждается довольно давно, написано много публикаций по этой теме, приняты международные стандарты, посвященные вопросам неотказуемости, в частности ISO/IEC 10181–4 и ISO/IEC 13888.

В нашей стране, до недавнего времени основными заказчиками систем информационной безопасности были государственные и военные структуры, для которых главной задачей обеспечения безопасности являлась защита от внешнего злоумышленника, т.е. проблемы неотказуемости отсекались полным доверием взаимодействующих сторон. Именно этим можно объяснить практическое полное отсутствие русскоязычного обсуждения неотказуемости. До сих пор даже нет устоявшегося общепринятого перевода термина non-repudiation на русский язык. Но вместе со становлением отечественного бизнеса возрастает потребность в защите электронных коммерческих взаимоотношений и проявляется всё больший интерес к неотказуемости, как неизбежной компоненте обеспечения информационной безопасности. Остаётся надеяться, что интерес будет иметь в качестве последствий не только слепое копирование западных стандартов, но и появление отечественных разработок в данной области, тем более что нельзя считать её полностью ясной на текущий момент. Многие аспекты неотказуемости, включая само её определение и место среди других услуг защиты, требуют дополнительного исследования и чёткого определения – неопределённость в этих вопросах чревата торможением развития многих перспективных отраслей современного бизнеса.

ЛИТЕРАТУРА:

1. ISO 7498–2. Information processing system – Open systems interconnection – Basic reference model – Part 2: Security architecture. International Organization for Standardization, 1989.
2. ГОСТ Р ИСО/МЭК 7498–2:99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

3. NIST Special Publication 800–26. Computer security.
4. FIPS Publication 191. Guideline for The Analysis Local Area Network Security. NIST, November 1994.
5. ISO/IEC 13888–1:2002. Information technology – Security techniques – Non-repudiation – Part 1: General.
6. Jianying Zhou and Dieter Gollmann. Observations on Non-repudiation. Lecture Notes in Computer Science 1163, Advances in Cryptology: Proceedings of Asiacrypt'96, pages 133–144, Kyongju, Korea, November 1996.
7. Jianying Zhou and Dieter Gollmann. Evidence and Non-repudiation. Journal of Network and Computer Applications, 20(3):267–281, July 1997.
8. ISO/IEC 10181–4. Information technology – Open system interconnection – Security frameworks in open systems – Part 4: Non-repudiation. ISO/IEC, 1996.

Получено 18.06.04. Опубликовано в Internet 12.09.04.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.25-26. Секция-6: Системы обнаружения вторжений.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/006)

МЕТОД КЛАСТЕРИЗАЦИИ МНОГОМЕРНЫХ СТАТИСТИЧЕСКИХ ДАННЫХ

Сапегин Л.Н.
ООО НПФ «Кристалл»

Для статистического анализа поведения субъекта в вычислительной системе могут использоваться методы кластеризации. В качестве анализируемого параметра метода может выступать любой набор числовых данных, представляющих собой числовую характеристику некоторых событий вычислительной системы, например: показание степени загруженности процессора, количество операций чтения и др. Количество видов анализируемых событий определяет размерность пространства, значением многомерного параметра является вектор чисел – числовых характеристик событий, снятых за единичный промежуток времени.

В общем случае, пусть дана совокупность многомерных статистических данных объема N, представленная N точками $X_i = (x_1^i, x_2^i, ..., x_n^i)$, $i = 1 \div N$ в n-мерном пространстве. Предполагается, что эта совокупность есть смесь некоторого числа выборок, каждая из которых имеет свой вероятностный закон распределения. Требуется разделить данную совокупность на выборки (кластеры) по принципу близости точек в смысле некоторого расстояния Евклида.

Предлагается составить матрицу (d_{ik}) попарных расстояний:

$$d_{ik} = \sqrt{\sum_{j=1}^{n} (x_j^i - x_j^k)^2} \; ; \; i, k = 1 \div N, \qquad (1)$$

где $d_{ii} = 0$, $i = 1 \div N$, и найти $d = \min_{i \neq k} d_{ik} > 0$, где d – минимальный шаг кластеризации.

Алгоритм кластеризации с шагом d разбивает совокупность точек X_i, i = 1-N, на подмножества (кластеры) $C_1^d, C_2^d, ...$ такие, что для всякой точки из C_1^d, если она там не единственная, найдется другая точка в C_1^d на расстоянии не более d; аналогично для C_2^d и т.д. Расстояния между любыми двумя кластерами больше d. Обозначим через $|C|$ - вес множества C, т.е. число точек в C. Тогда, очевидно, $|C_1^d| + |C_2^d| + \ldots = N$.

Алгоритм кластеризации с нормой $2d$ приведет к увеличению весов кластеров и к уменьшению их числа при сохранении суммы весов, равной N: $|C_1^{2d}| + |C_2^{2d}| + \ldots = N$.

Результаты кластеризации с шагом ld, $l = 1, 2, 3, \ldots$ будем располагать в таблице 1 в порядке убывания весов кластеров: $|C_1^{ld}| \geq |C_2^{ld}| \geq |C_3^{ld}| \geq \ldots \geq |C_{s_l}^{ld}|$, где s_l – число кластеров. Тогда $s_1 \geq s_2 \geq s_3 \geq \ldots$ и $|C_1^d| \leq |C_1^{2d}| \leq |C_1^{3d}| \leq \ldots$

Таблица 1 – Веса кластеров на каждом шаге кластеризации

Норма	Веса кластеров						
D	$\left\|C_1^d\right\|$	$\left\|C_2^d\right\|$	…	…	…	$\left\|C_{s_1}^d\right\|$	…
2d	$\left\|C_1^{2d}\right\|$	$\left\|C_2^{2d}\right\|$	…	…	$\left\|C_{s_2}^{2d}\right\|$	…	…
…	…	…	…	…	…	…	…

Покажем, как вычисляется любая строка таблицы 1 для кластеризации с произвольным шагом $h \geq d$.

По заданному h в матрице (d_{ik}) помечаются те элементы, которые не превосходят h. Числовые значения d_{ik} после этого не имеют значения для кластеризации с шагом h.

Выписываем серии номеров помеченных элементов в строках матрицы следующим образом.

Первая серия состоит из одного номера 1.

Из строки 1 выбираем номера помеченных элементов 1, a_1, a_2, … и удаляем номер 1, поскольку он уже есть в первой серии.

Вторая серия: a_1, a_2, ….

Если вторая серия пуста, то точка X_1 составляет первый кластер веса 1. Все пометки в строке 1 и столбце 1 удаляются. Первая серия следующего кластера состоит из одного номера 2 и далее, как описано выше.

Если вторая серия не пуста, то из строк $a_1, a_2, \ldots$ выбираем номера помеченных элементов: b_1, b_2, …; c_1, c_2, … и удаляем все номера, которые уже встречались ранее в сериях выше или в этой строке. Оставшиеся номера обозначим через $\overline{b_1}, \overline{b_2}, \ldots; \overline{c_1}, \overline{c_2}, \ldots$.

Третья серия: $\overline{b_1}, \overline{b_2}, \ldots; \overline{c_1}, \overline{c_2}, \ldots$.

Если третья серия пуста, то точки $\{X_1, X_{a_1}, X_{a_2}, \ldots\}$ составляют первый кластер. Все пометки в строках и столбцах с номерами 1, a_1, a_2, … удаляются. Первая серия следующего кластера состоит из одного номера, отличного от 1, a_1, a_2, … и далее, как описано выше.

Если третья серия не пуста, то из строк $\overline{b_1}, \overline{b_2}, \ldots; \overline{c_1}, \overline{c_2}, \ldots$ выбираем номера помеченных элементов и удаляем из них все номера, которые уже встречались ранее в сериях выше или в этой строке. Оставшиеся номера составляют четвертую серию.

Выделение очередного кластера завершается после получения пустой серии путем объединения предшествующих непустых.

Удаление последних помеченных элементов в матрице (d_{ik}) указывает на то, что все кластеры выделены.

Итак, предполагается, что каждый кластер отображает определенную роль, выполняемую субъектом при работе в вычислительной системе. Поскольку каждый субъект, как правило, меняет свои роли достаточно часто, то данные мониторинга одного субъекта являются смесью в неизвестных пропорциях выборок от различных ролей. Кластеризация позволяет разделить данные мониторинга не по субъектам, а по ролям, исполняемым субъектом или совокупностью всех субъектов.

Получено 24.06.2004. Опубликовано в Internet 20.10.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.27-30. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/007)

РАСЧЕТ ЧИСЛА КОМБИНАЦИЙ В ХОРОШО ЗАПОМИНАЕМЫХ НЕСЛУЧАЙНЫХ БИОМЕТРИЧЕСКИХ ПАРОЛЯХ

Чернов Е.О., Глухов Д.Н., Капитуров Н.В., Иванов А.И.
Пензенский государственный университет, ПНИЭИ

В настоящее время активно идут процессы информатизации современного общества. Будущее информационное общество можно сделать устойчивым, только используя массовую криптографическую защиты как частной, так и государственной информации и информационных потоков. Технически это осуществимо уже сейчас, однако при переходе к массовой криптографии резко обостряется проблема хранения личных ключей массой пользователей. Международная криптографическая общественность в лице ISO/IEC SC27 видит решение этой задачи в использовании биометрии. Необходимо создать недорогие и высоконадежные механизмы надежного хранения криптографических ключей с биометрическим доступом к ним. Лидерами по разработке такого типа механизмов преобразования нечеткого, нестабильного биометрического образа человека в его личный ключ является Россия [1] и США [2].

В России развивается биометрико-нейросетевой подход, построенный на преобразовании тайного рукописного или голосового пароля в тайну личного ключа пользователя. При этом становится очевидным, что изначальное число комбинаций биометрического пароля (рукописного или голосового) входит как некоторый базовый коэффициент в расчеты по оценке мощности входного множества многомерных континуумов входных биометрических данных, которые преобразуются заранее обученной искусственной нейронной сетью в личный ключ пользователя или белый шум.

Следует отметить, что расчет числа комбинаций биометрического пароля, состоящего из случайных знаков и символов не представляет особого труда. Однако такие биометрические пароли бесперспективны, так как трудны для запоминания пользователями и в конечном итоге оказываются гораздо более слабыми, чем неслучайные хорошо запоминаемые и потому длинные биометрические пароли.

При расчетах как основа был взят Русский орфографический словарь РАН [1], который в виде текстовых файлов размещен в Internet (http://dict.csb.lv/data/). Средствами JavaScript были построены поисковые машины, извлекающие из этого словаря осмысленные слова с разным числом букв, имеющие отличия хотя бы в одной букве.

В конечном итоге поисковые машины разбили базовый словарь [3] из 157 тысяч слов на 36 групп осмысленных слов. Наибольший интерес для расчетов представляют группы слов, состоящих из более чем двух букв, но не превышающих 21 букву.

Данные по численности этих групп приведены в таблице 1.

Таблица 1

Число букв в слове (N группы)	Число слов в группе		Число букв в слове (N группы)	Число слов в группе
1	15		12	15094
2	166		13	11321
3	890		14	8330
4	2357		15	5804
5	5138		16	4019
6	8160		17	2693
7	12707		18	1881
8	17362		19	1206
9	19701		20	759
10	19975		21	518
11	17920		22….36	1033
Число букв в слове (N группы)	Число слов в группе		Число букв в слове (N группы)	Число слов в группе

Исходя из таблицы 1, мы можем вычислить вероятность удачной атаки подбора неслучайного рукописного (голосового) пароля, зная число букв его образующих, однако такие расчеты будут неверны из-за того, что русский орфографический словарь далеко не полон (он не учитывает размножение число слов из-за особенностей морфологии разговорного русского языка).

Учесть подобные модификации слов можно статистически в виде графа, отражающего коэффициенты размножения групп слов и их коэффициент размножающего переноса в соседние группы с близким числом букв. Подобный граф был построен на случайной выборке их 200 слов и приведен на рисунке 1.

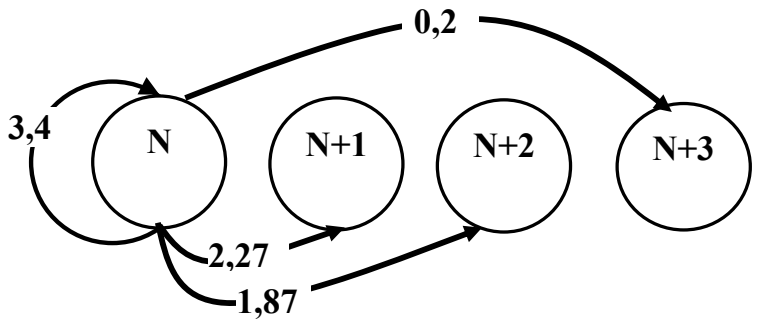


Рисунок 1. – Граф статистических связей, отражающий коэффициент размножения групп слов и коэффициенты размножающего переноса в соседние группы

Приведенный выше граф связей позволяет проследить увеличение числа реальных слов содержащих заданное число букв. Результаты подобных расчетов сведены в таблицу 2.

Таблица 2

Число букв (N группы)	Число слов в группе
2	604
3	3502

4	10730
5	25530
6	46200
7	75320
8	10960
9	13930

Очевидно, что число осмысленных слов русского языка с учетом их морфологии оказывается существенно больше числа слов изначального орфографического словаря [3].

Еще одним обстоятельством, приводящим к росту числа слов в группах расчета является то, что в биометрических паролях нет возможности точного указания соответствия числа букв в слове пароле и, соответствующего, числа входов нейросети. Сегодня используются далеко не совершенные автоматы, дробящие рукописный или голосовой пароль на учитываемые фрагменты. Кроме того почерки у всех различны, что так же сказывается на качестве дефрагментации. В конечном итоге получается, что по числу входов искусственной нейронной сети нельзя точно установить число букв входного биометрического пароля. Возможно только предположительное утверждение о том, что биометрический пароль относится к группам слов состоящих из 2,3,4 букв или 3,4,5 букв, 4,5,6 букв и так далее.

В результате для биометрических паролей мы приходим к необходимости представления их по 8 наиболее интересным группам, число слов к которых дано в таблице 3.

Таблица 3.

N группы	Число букв в слове, принадлежащем группе	Число слов в группе
1	2,3,4	14398
2	3,4,5	39762
3	4,5,6	82460
4	5,6,7,	147050
5	6,7,8	231120
6	7,8,9	324220
7	8,9,10	405000
8	9,10,11	450600

Следует подчеркнуть, что для человека легко запоминаемыми являются осмысленные словосочетания. В частности как биометрические пароли людьми могут быть использованы сочетания из двух слов. В этом случае число сочетаний в таких составных биометрических паролях резко увеличивается, что и нашло отражение в таблице 4.

Число сочетаний сложного пароля из двух слов – Таблица 4

Сочетания слов, принадлежащих к разным группам	1-ое слово 1 группа	1-ое слово 2 группа	1-ое слово 3 группа	1-ое слово 4 группа	1-ое слово 5 группа	1-ое слово 6 группа	1-ое слово 7 группа	1-ое слово 8 группа
2-ое слово 1 группа	2.07*e+8	5.72*e+8	1.19*e+8	2.12*e+8	3.33*e+8	4.67*e+8	5.83*e+8	6.49*e+8

2-ое слово 2 группа	5.72*e+8	1.58*e+9	3.28*e+9	5.85*e+9	9.19*e+9	1.29*e+9	1.61*e+9	1.79*e+9
2-ое слово 3 группа	1.19*e+9	3.28*e+9	6.80*e+9	1.21*e+9	1.91*e+9	2.67*e+9	3.34*e+9	3.72*e+9
2-ое слово 4 группа	2.12*e+9	5.85*e+9	1.21*e+9	2.17*e+9	3.40*e+9	4.77*e+9	5.96*e+9	6.63*e+9
2-ое слово 5 группа	3.33*e+9	9.19*e+9	1.91*e+10	3.40*e+10	5.34*e+10	7.49*e+10	9.36*e+10	1.04*e+11
2-ое слово 6 группа	4.67*e+9	1.29*e+10	2.67*e+10	4.77*e+10	7.49*e+10	1.05*e+11	1.31*e+11	1.46*e+11
2-ое слово 7 группа	5.831*e+9	1.61*e+10	3.34*e+10	5.96*e+10	9.36*e+10	1.31*e+11	1.64*e+11	1.82*e+11
2-ое слово 8 группа	6.49*e+9	1.79*e+10	3.72*e+10	6.63*e+10	1.04*e+11	1.46*e+11	1.82*e+11	2.03*e+11

Таким образом, легко запоминаемые людьми составные биометрические пароли из двух слов на рисунке имеют число комбинаций сопоставимое длинными случайными паролями, состоящими из 8, 9 случайных знаков. Запомнить случайные пароли из 8, 9 случайных знака для большинства людей крайне сложно и они идут на нарушения, записывая их, например, на бумаге. Иначе обстоит дело с осмысленными паролями из обычных слов русского языка. Люди легко запоминают достаточно длинные пароли такого типа из 2, 3, 4 слов. Как следствие, стойкость хорошо запоминаемых биометрических паролей может быть сделана на несколько порядков более высокой в сравнении с классическими паролями из случайных символов. При этом аутентификация человека по его биометрическому паролю остается дружественной даже при использовании паролей из нескольких логически связанных слов, цифр, знаков. Для человека не составляет особого труда запомнить и воспроизвести понятную ему парольную фразу, даже если эта фраза достаточно длинная.

ЛИТЕРАТУРА:

1. Иванов А.И. Объединение протоколов аутентификации //Защита информации. Конфидент, 2002 г., №1, с 64–69.
2. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data /Yevgeni Dodis, Leonid Reyzin, Adam Smith //April 13, 2004. www.cs.bu.edu/~reyzin/fuzzy.html
3. Русский орфографический словарь Российской академии наук. Отв. Редактор В.В. Лопатин. М.: Азбуковник, 2000 г.

Материалы поступили 12.07.2004. Опубликовано в Internet 12.09.2004

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.31-33. Секция-6: Системы обнаружения вторжений.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/008)

ИССЛЕДОВАНИЕ МЕТОДА КЛАСТЕРИЗАЦИИ МНОГОМЕРНЫХ СТАТИСТИЧЕСКИХ ДАННЫХ

Лакин К.А.
ООО НПФ «Кристалл»

Статистический анализ поведения субъекта в вычислительной системе включает в себя широкий спектр методов анализа данных мониторинга (аудита) поведения субъекта, в том числе, и методов добычи данных. Стоит отметить, что большинство методов статистического анализа требует значительных вычислительных ресурсов, и используемые статистические данные должны иметь достаточно большой объем. Тем не менее, методы классической статистики являются на сегодня единственным корректным и хорошо изученным инструментом анализа поведения субъекта в вычислительной системе.

В данной статье рассматривается применимость методов кластерного анализа на примере метода кластеризации, описанного в [1], к разбору и анализу данных мониторинга и, следовательно, к анализу поведения субъекта в вычислительной системе. Предложенный в [1] метод кластеризации многомерных статистических данных имеет целью эффективный поиск простых, но понятных моделей, которые могут интерпретироваться как интересные (в первую очередь администратору безопасности вычислительной системы) и полезные знания. Здесь намеренно сделан упор на термин «знание», так как результатом кластерного анализа являются не только числовые данные в отличие от большинства методов статистического анализа, где результатом, как правило, является числовая оценка. Ниже будет это показано.

Условия проводимых экспериментов были следующими:

– метод анализа: метод кластеризации многомерных статистических данных;

– данные для анализа: данные от штатной системы регистрации событий ОС Novell NetWare;

– входные данные: набор точек, представляющих активность пользователя в течении суток по часам.

В процессе экспериментов по применению кластерного анализа было выявлено, что кластеризация многомерных статистических данных может выступать как:

– фильтр, способный уменьшить количество ложных срабатываний статистических методов;

– средство для распознавания выполняемых ролей исполняемых субъектом;

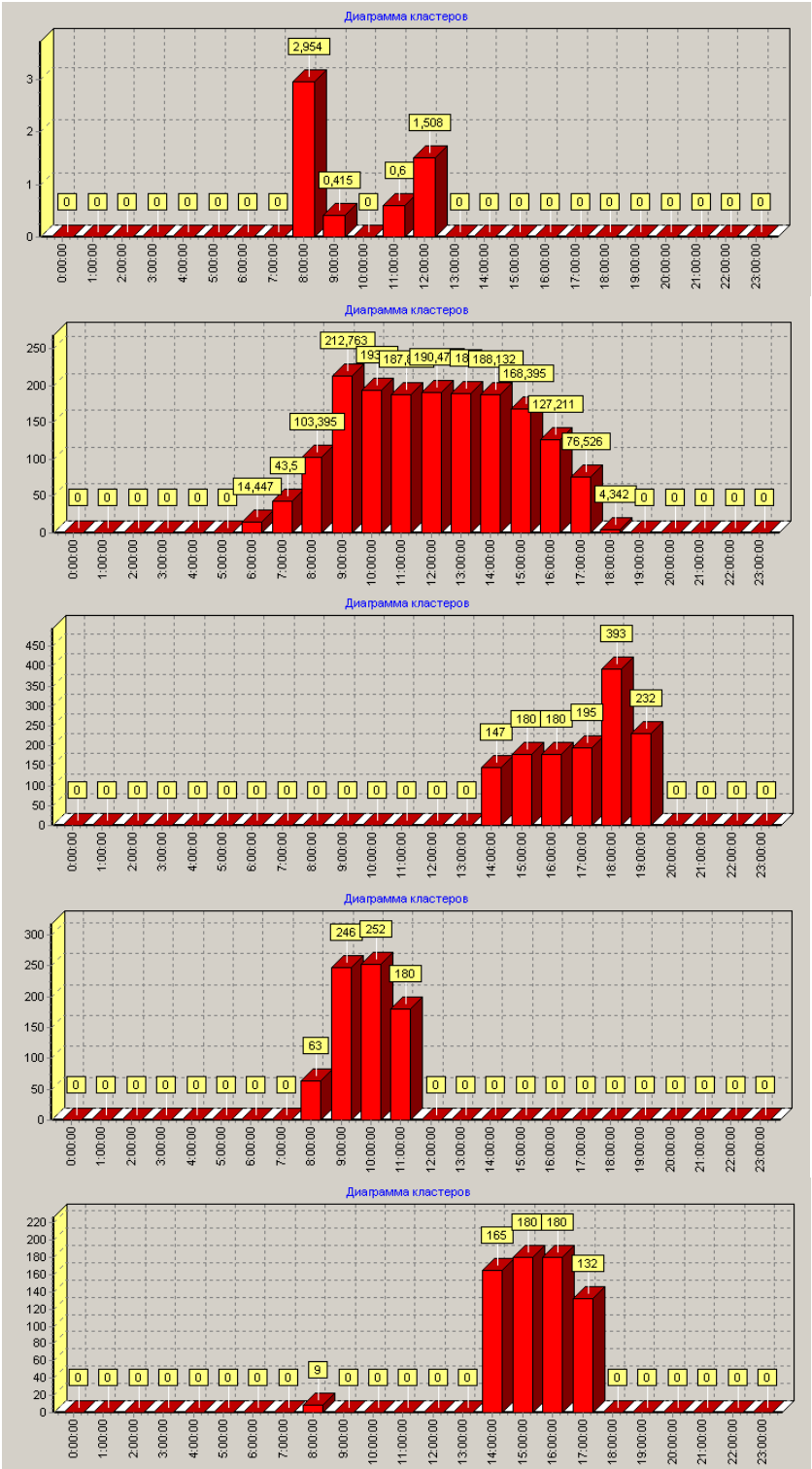
– средство для выявления нетипичной активности субъекта.

Рассмотрим конкретный пример применения данного метода. Например, пусть заданы следующие параметры:

– интервал анализа – 104 дня (включая выходные и праздничные дни);

– входной анализируемый параметр – количество модификаций файлов субъектом ПОЛЬЗОВАТЕЛЬ.

В итоге было получено знание, которое содержит информацию о пяти обнаруженных кластерах. Вид центров полученных кластеров приведен на рисунке 1.



Центр кластера 1. Количество точек в кластере – 65.

Центр кластера 2. Количество точек в кластере – 38.

Центр кластера 3. Количество точек в кластере – 1.

Центр кластера 4. Количество точек в кластере – 1.

Центр кластера 5. Количество точек в кластере – 1.

Рисунок 1 - Вид центров полученных кластеров

Под центром кластера понимается точка, значение координат которой являются средним значением по отношению ко всем точкам кластера.

Анализируя полученные кластеры (например, с помощью других статистических методов), вероятнее всего можно ожидать снижение числа

ложных срабатываний статистических методов. Также можно прийти к выводу о двух ролевых составляющих поведения данного субъекта (так как явно из рисунка 1 видно наличие двух особо выраженных кластеров) и о выявлении трех образцов нетипичного поведения.

В дальнейшем полученную информацию (знание) можно использовать для более качественного построения эталонов поведения субъекта (их количество теперь может быть два, так как выявлены две ролевые составляющие), что приведет к уменьшению количества ложных срабатываний. Также возможно применение данного метода для поиска нетипичного поведения с помощью метода определения принадлежности точки многомерной выборке [2], который не требует наличия большого объема данных.

Стоить отметить, что место метода кластеризации в процессе анализа поведения субъекта в вычислительной системе, возможно, должно находиться перед выбором статистических методов. Метод кластеризации является источником данных для статистических и иных методов оценки поведения субъекта в вычислительной системе.

Также стоит отметить трудность настройки данного метода. В процессе экспериментов выяснилось, что нельзя использовать одинаковые настроечные параметры для всех субъектов.

Таким образом, применение метода кластеризации многомерных статистических данных может позволить найти новые источники данных, распознать выполняемые роли субъектом, уменьшить количество ложных срабатываний, что несомненно приведет к понижению размерности задачи оценки поведения субъекта в вычислительной системе.

ЛИТЕРАТУРА:

1. Сапегин Л.Н. Метод кластеризации многомерных статистических данных. Труды научно-технической конференции под редакцией Волчихина В.И., Зефирова С.Л., Иванова А.И. Т.5 – Пенза: Издательство Пензенского научно-исследовательского электротехнического института, 2005, стр. 25–26.
2. Лакин К.А., Сапегин Л.Н. Способ определения принадлежности точки многомерной выборке. Труды научно-технической конференции под редакцией Волчихина В.И., Зефирова С.Л., Иванова А.И. Т.4 – Пенза: Издательство Пензенского научно-исследовательского электротехнического института, 2004, стр. 49–53.

Получено 16.07.04. Опубликовано в Internet 12.09.04.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.34-38. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/009)

ОЦЕНКА СЛОЖНОСТИ ЗАДАЧИ РАСПОЗНАВАНИЯ РУКОПИСНЫХ СИМВОЛОВ КИРИЛЛИЧЕСКОГО АЛФАВИТА

Демьянов А.Е., Глухов Д.Н., Капитуров Н.В., Иванов А.И.
Пензенский государственный университет, ПНИЭИ

В настоящее время карманные компьютеры не имеют клавиатуры. Клавиатура либо эмулируется на чувствительном экране наладонника, либо используется программа распознавания рукописно вводимых букв. Существует несколько вариантов таких программ, обеспечивающих примерно одинаковые статистические характеристики распознавания. Эти программы реализованы на методах классической статистической обработки и ориентированы на почерк среднестатистического пользователя. Реальных статистических данных, позволяющих оценить вероятности ошибок существующих программ распознавания рукописных букв их производители не приводят. Самостоятельное тестирование этих программ дает крайне неудовлетворительные результаты. Вероятность ошибки при распознавании похожих символов составляет порядка 0.08.

Столь высокая вероятность ошибок обусловлена несовершенством механизмов распознавания рукописных букв, заложенных в продаваемом сегодня программном обеспечении. Одним из путей совершенствования механизмов распознавания является переход к решению задачи в нейросетевом базисе. При этом имеет смысл заранее оценить сложность задачи разделения тех или иных рукописных символов или сложность задачи выделения конкретного символа из хаоса всех возможных рукописных символов и знаков.

Для оценки сложности распознавания рукописных символов использовалась программа «Нейропреподаватель», ранее созданная в Пензенском государственном университете для проведения лабораторных работ по курсу «Нейросети». Использовались однослойные нейросети с чётной и нечётной формой разделяющей классы образов нелинейности. Средствами той же программы были созданы образы рукописных символов для всех букв кириллического алфавита, которые сохранялись в файлах примеров средствами ПО «Нейропреподаватель». После чего выполнялось обучение нейросети каждому из примеров.

Монотонно уменьшая (или увеличивая) нижний порог качества учитываемых входных параметров, мы добились наилучшего качества обучения искусственного нейрона. На рисунке 1 показан пример обучения нейросети с чётной формой нелинейности, где отображены нормальные законы распределения значений на выходах нейросети, соответствующие выделяемому множеству с центром – m_1 и множеству всех иных рукописных букв с центром – m_2.

Очевидно, что чем уже выделяемое множество тем легче его отделить от образов иных рукописных букв. Качество выделяемости – q [1] для каждого конкретного рукописного символа принимает свое значение. Исходя из этого можно вычислить значения показателя качества – q и руководствуясь им взаимно упорядочить рукописные символы по их качеству выделяемости. Для рукописного почерка студента Демьянов А.Е. полученные данные сведены в таблицу 1. Из таблицы 1 видно, что проще всего выделяется буква «Ф». Наиболее трудной для выделения является буква «Ю». Кроме показателя качества в

таблице 1 дается число учитываемых параметров и нижний порог качества, по которому параметры принимаются к учету.

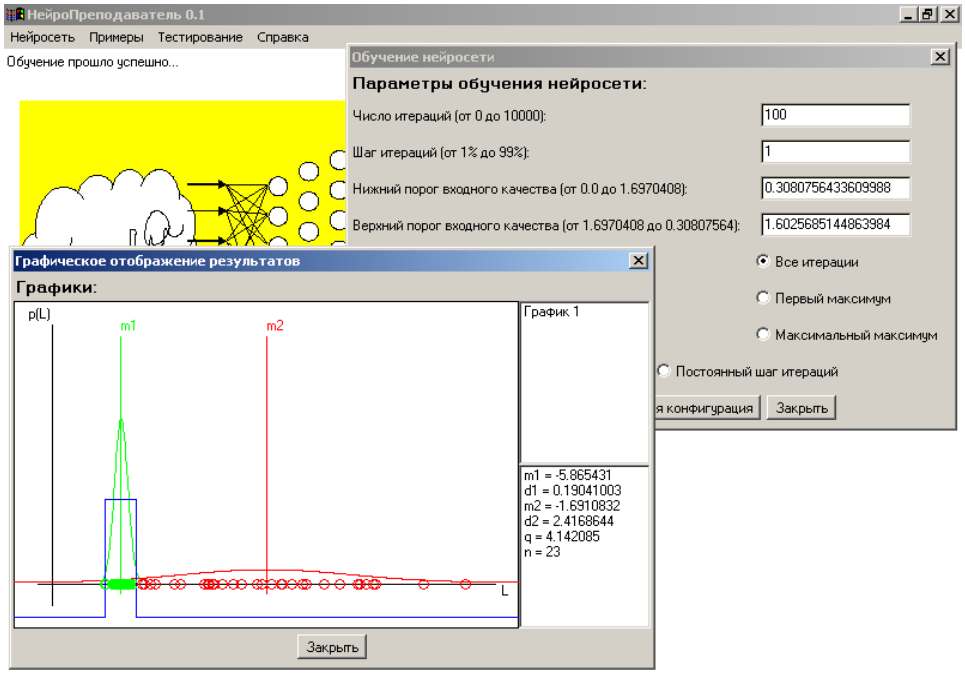


Рисунок 1 - Пример результата обучения нейросети с чётной формой нелинейности

При обучении однослойной нейросети и формировании данных таблицы 1 проводилась оптимизация учитываемых параметров, параметры с очень низким качеством отбрасывались.

Таблица 1

Буква	Данные для сети с чётной нелинейностью			Буква	Данные для сети с чётной нелинейностью		
	Значение q	Число параметров n	Нижний порог по качеству		Значение q	Число параметров n	Нижний порог по качеству
ф	4.388843	21		л	2.6921043	12	
з	3.692223	15		ц	2.5973427	7	
д	3.5891576	42		ь	2.582907	53	
й	3.5005162	20		т	2.534781	13	
у	3.4713695	15		щ	2.4753187	18	
ё	3.399528	16		н	2.4169106	6	
ж	3.200658	19		п	2.372962	37	
в	3.1345468	18		б	2.3678172	11	0,4422
ъ	3.041315	17		м	2.297085	40	
ы	3.040803	50		р	2.2902355	15	
ш	2.970213	26		ч	2.288431	8	
с	2.96102	10		е	2.2868278	12	
и	2.9488966	8		к	1.972176	10	
э	2.9190598	15		г	1.682608	6	
о	2.89446314	15		х	1.6744571	27	
я	2.8836718	33		ю	1.3621398	67	
а	2.737236	42					

В случае использования нечетных пороговых нелинейных функций показатели качества оказываются иными и, соответственно, возникает иная упорядоченность рукописных символов по трудности их выделения. Пример использования нечетной разделяющей функции дан на рисунке 2.

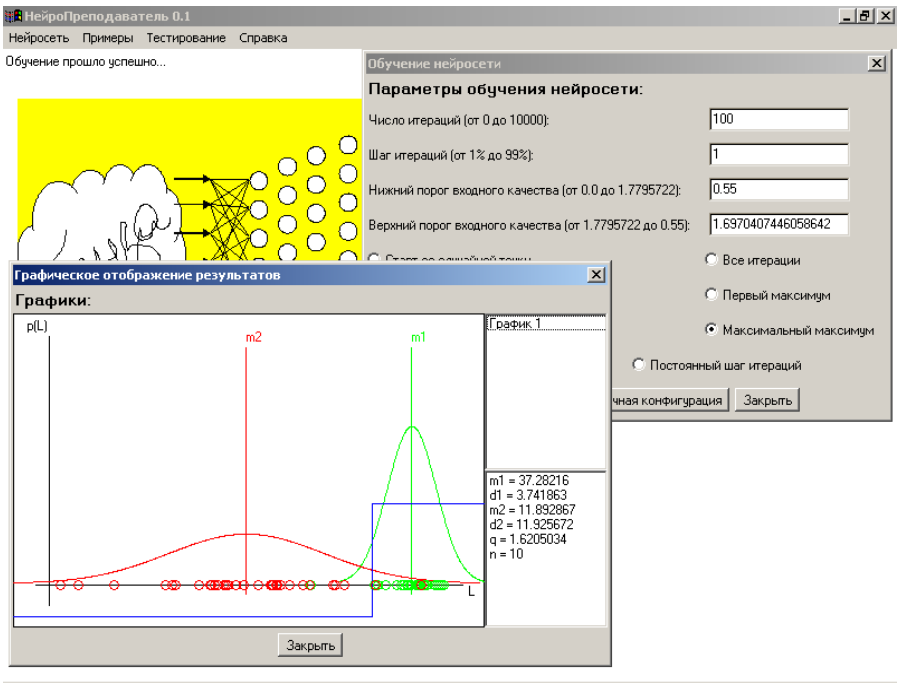


Рисунок 2. – Результат обучения нейросети с нечётной разделяющей нелинейностью на выходе

Данные по качеству обучения нейросети с нечётной формой нелинейности приведены в таблице 2.

Таблица 2

Буква	Данные для сети с нечётной нелинейностью			Буква	Данные для сети с нечётной нелинейностью		
	Значение q	Число параметров n	Нижний порог по качеству		Значение q	Число параметров n	Нижний порог по качеству
ф	3.1431017	35	0.44	ш	1.7899579	26	
й	2.8955355	20	0.48	ь	1.7826998	22	
ё	2.710481	21	0.415	с	1.7772765	22	
з	2.2630718	10		х	1.773411	22	0.34
ы	2.0708885	36	0.35	щ	1.6205034	10	0.55
д	2.0559483	18		к	1.5508748	15	
т	2.039105	26		ч	1.4964478	12	0.5
ж	2.0275903	40		ц	1.4715246	7	0.58
л	1.9726379	24		р	1.4240022	16	
м	1.9672048	39		н	1.3514788	13	
ъ	1.9381046	16	0.47	е	1.3201332	10	
п	1.9178623	26		б	1.2883855	31	
я	1.8861287	45		ю	1.2548362	28	0.33
у	1.8529338	40	0.295	о	1.2198315	24	
и	1.8424624	19		э	1.1236372	12	0.36
в	1.8197958	16		г	0.9001135	17	
а	1.7981689	58	0.31				

Нетрудно убедиться в том, что данные таблиц 1 и 2 оказываются сопоставимыми. В частности для рассматриваемого рукописного почерка выделение буквы «Ю» относится к наиболее сложным задачам, как по шкале четного качества, так и по шкале нечетного качества. Напротив выделение буквы «Ф» оказывается самой простой задачей.

Следует подчеркнуть, что в таблицах 1 и 2 даны только предварительные результаты упорядочивания рукописных символов по качеству их выделения. Приведенные данные должны быть дополнены характеристиками отделимости каждой конкретной буквы от ближайших к ним рукописных образов. Например, для буквы «Ю» ближайшим соседом с права является буква «Т», а ближайшим соседом с лева является буква «Й» (смотри рисунок 3).

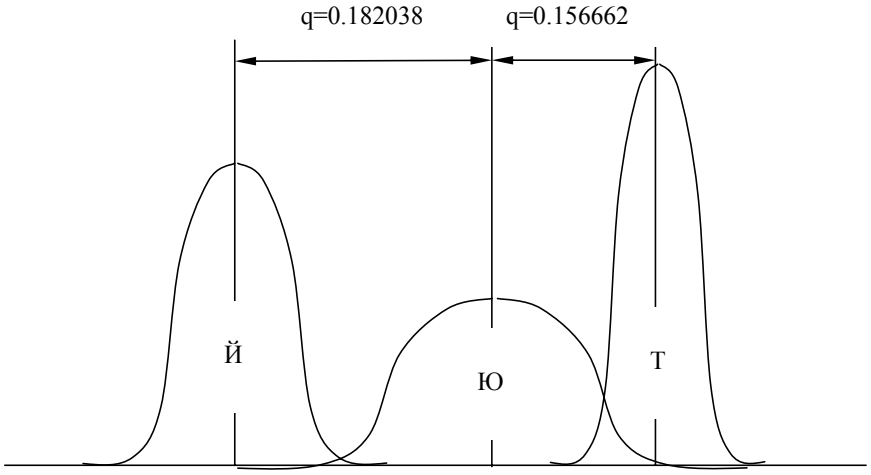


Рисунок 3. – График удалённости образа от его ближайших соседей.

Очевидно, что для ближайших соседей могут быть вычислены соответствующие показатели качества – q. Полученные результаты по отделимости той или иной буквы от ближайших соседей для наиболее плохих символов сведены в таблицу 3.

Таблица 3

Буква	**ф**	**а**	**ю**	**щ**	**й**
Ближайший сосед слева	я (-0.378936)	н (-0.592693)	й (-0.1820389)	м (-1.0256449)	о (-1.848594)
	ё (-0.726496)	м (-0.829608)	ы (-0.5534471)	т (-1.3721308)	и (-2.048364)
Ближайший сосед справа		я (1.1186044)	т (0.1566623)		
			щ (0.3027493)		

В таблице 4 для всех рукописных букв кириллического алфавита приведены по два ближайших соседа с правой стороны и с левой стороны. Хотя данные получены для почерка одного человека они в первом приближении могут рассматриваться как оценки соответствующие среднестатистическим характеристикам почерков. Выборочные проверки полученных данных на других почерках дают похожие результаты.

Таблица 4

Буква	Ближайшие соседи слева		Ближайшие соседи справа			Буква	Ближайшие соседи слева		Ближайшие соседи справа	
а	н	м	я	-		р	м	ш	-	-
б	и	н	-	-		с	з	а	г	о
в	б	г	е	ъ		т	ш	м	и	ы
г	й	н	з	е		у	з	д	р	г
д	у	ч	-	-		ф	я	ё	-	-
е	п	г	щ	-		х	к	о	н	л
ж	ы	ч	э	-		ц	я	ч	у	м
з	г	щ	д	е		ч	ц	д	к	а
и	н	ч	ж	м		ш	ы	м	ш	ж
й	о	и	-	-		щ	ы	т	-	-
к	т	с	в	р		ъ	ъ	р	ч	я
л	ш	ы	м	п		ы	м	ш	р	ф
м	н	т	-	-		ь	е	ж	ъ	э
н	и	м	б	ж		э	а	г	о	п
о	в	с	к	б		ю	й	ы	т	щ
п	м	и	ы	л		я	а	к	-	-

Пользуясь приведенными выше данными можно еще до решения задачи распознавания рукописных почерков в нейросетевом базисе оценить ее сложность и ориентировочно дать рекомендации по выбору топологии нейросети.

ЛИТЕРАТУРА:

1. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. //Монография. Пенза. Изд-во ПГУ, 2000 г. – 188 с. (http://beda.stup.ac.ru/biometry).

Получено 31.08.2004. Опубликовано в Internet 20.10.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.39-48. Секция-1: Концептуальные основы информационной безопасности и проблемы информационного противоборства
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/010)

ТИПОВЫЕ ПОДХОДЫ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Каминский В.Г.
НПФ «Кристалл» (г. Пенза)

В данной статье приводится обобщенный материал по наиболее распространенным методам, способам и принципам оценки рисков информационной безопасности и излагается пример подход по их возможной классификации

Как правило, нормативно-юридическая основа процесса оценки риска базируется на документах, стандартах, положениях, официально принятых на уровне государства, отрасли или организации, что позволяет официально признать их юридический статус для закрепления возможности их использования в целях проведения тех или иных работ, в том числе и работ по оценке риска. При отсутствии официального принятия документов исчезает обоснованность и мотивация действий персонала управления (менеджеров различного уровня), связанных с использованием результатов оценки рисков и принятых решений, а также становится неясным статус результатов таких оценок рисков информационной безопасности (ИБ).

Нормативно-техническая основа процесса оценки базируется на документах, которые выступают в качестве технического руководства, которому должны следовать при оценках рисков ИБ для автоматизированных систем (АС), информационных технологий (ИТ) или организации, для учета потребностей бизнеса организации и технических деталей оценки рисков.

Ниже в таблице 1 приведен перечень наиболее распространенных продуктов, методов и способов оценки рисков, их юридический статус, техническая основа для оценки и предполагаемый статус результатов оценки. Более подробная информация по ним может быть получена из ряда источников [1] – [14] Как видно из представленной в таблице информации, как правило, в качестве юридической основы оценки лежит принятый в государстве (например, URSIT в США, CRAMM в Великобритании) или в сообществе (например, MARION в банковском сообществе Франции, ISO TR 13569 в банковском мировом сообществе) документ в виде положения или стандарта.

Таблица 1 – Перечень продуктов, методов и способов оценки рисков

Наименование	Статус	Техническая основа оценки	Результат оценки
URSIT (метод)	Принят для оценки рисков ИТ финансовых организаций и провайдеров ИТ-услуг для надзорных органов США	Принят ФРС США и учитывает специфику банковского дела при оценка ИТ финансовых организаций и провайдеров ИТ-услуг для банковской сферы	Выявление организаций и провайдеров услуг с высоким риском с целью усиления к ним мер надзорного характера
OCTAVE (метод)	Рекомендации, разработанные Институтом	Самоуправляемая сводной группой анализа оценка	Выявление организацией рисков ИБ в виде рисков

Наименование	Статус	Техническая основа оценки	Результат оценки
	Разработки Программного обеспечения Carnegie для широкого применения	рисков ИБ организаций	конфиденциальности, целостности и доступности активов ИТ
ISO TR 13569 (пример подхода)	Технический отчет, принятый техническим комитетом ИСО 68 «Банковские и связанные с ними финансовые услуги»	В первичной основе рекомендован для применения в банковской сфере. Содержит пример применения для банковского сообщества одного из методов оценки рисков, определенных в 3-части ISO/IEC 13335	Детализированная оценка рисков: – денежной потери; – потерь производительности; – системных затруднений, – при использовании АС и ИТ в банковской сфере
COBIT (пример подхода)	Принят Фондом Аудита и Контроля Информационных систем	Определены 34 процесса и соответственно целей контроля ИТ организации не привязанные к области деятельности организации. Один из процессов планирования и организации 9 определяет обобщенный процесс оценки рисков.	Содержит общие рекомендации по оценке рисков на этапе планирования применения в организации систем ИТ
MARION (метод)	Разработан Банковской комиссией Франции, рекомендательно принят для оценки состояния информационных систем кредитный организаций	Документ принят в качестве основы для оценки рисков ИБ для ИС кредитных организаций Франции по 25 областям по 4-х бальной шкале для каждой области	Выявление наиболее проблемных областей для возможной последующей проработки этих направлений.
CRAMM (программный продукт)	Метод анализа и контроля рисков, принят Центральным Агентством по Компьютерам и Телекоммуникациям (CCTA) Великобритании в поддержку стандарта BS7799	Как метод принят в Великобритании для оценки рисков в различных отраслях деятельности	Оценка рисков ИБ организации при обработке критической информации
ISO/IEC 17799 (философия)	Международный стандарт	Используется отдельными методами оценки рисков в качестве образца «нулевого риска», где риск означает степень отклонения от образца	При признании такого подхода используется как руководство к действию по тем областям ИБ, где выявлены существенные отклонения от ISO/IEC 17799

Наименование	Статус	Техническая основа оценки	Результат оценки
ISO/IEC 13335 (пример подхода)	Технический отчет ИСО и МЭК	Определяет в 3 части 4 различных подхода к оценке рисков безопасности ИТ, методологически подобных тем, что реализованы в CRAMM	Оценка риска организаций и ИТ по одному из приведенных в отчете методов оценки рисков
COBRA	(программный продукт)	Оценка рисков как степень отклонения от образца - международного стандарта ISO/IEC 17799	Степень отклонения от положений (рекомендаций) ISO/IEC 17799
РД 4.25.01-93	Действует в России	Документ ориентирован на оценку состоятельности и качества продукции, для оценки риска, может быть использован только методологически	Оценка состоятельности и качества выпускаемой продукции на основе сравнения с выбранным ближайшим аналогом (образцом), определяет степень отклонения от образца
Принципы менеджмента риска для электронных банковских услуг (Базельский комитет по банковскому надзору)	Рекомендован международной банковской организаций для применения в банковских структурах.	Ориентирован на банковскую специфику и рассматривает вопросы безопасности при использовании ИТ в банковских организациях	На результат оценки непосредственно не ориентирован
ГОСТ Р ИСО/МЭК 15408-2002 (пример подхода)	Введен в действие в России с начала 2004 г.	Общетехнический стандарт по безопасности ИТ, где показаны место и роль оценок рисков к общей концепции безопасности ИТ. Для практики рекомендует руководствоваться положениями ISO/IEC 13335	Включение в ПЗ и ЗБ актуальных угроз безопасности ИТ и выбор необходимых функциональных требований и требований доверия безопасности ИТ

Определение технической основы процесса оценки позволяет выбрать образец (например, разработчиками программного продукта COBRA был выбран в качестве образца международный стандарт ISO/IEC 17799), или определить перечень требований (например, URSIT), или общую методологию (например, предложения Базельского комитета по банковскому надзору). В любом случае происходит конкретизация позиций, выполнение проверок по которым, например, по степени отклонения от них, позволяет прийти к оценке риска.

В связи с этим становится понятным и ясным результат такой оценки риска, который как видно из таблицы 1 может быть:

- оценкой на соответствие выбранному образцу;
- оценкой на основе анализа угроз информационным активам, с учетом уязвимостей объектов защиты.

Одновременно следует отметить, что непосредственно статистические методы оценки в практике работы международного сообщества применения не нашли. Однако статистические меры широко используются в качестве основы и обоснования выбора перечня угроз и вероятностей их реализации, а также оценки предполагаемого ущерба при их реализации.

Учитывая многообразие методов и подходов, применяемых при оценке рисков, представляется целесообразным на основании приведенной информации сформулировать перечень возможных типовых подходов, которые могут быть использованы при оценке рисков. Как любая классификация такое представление материалов позволяет определить, а в дальнейшем, возможно, утвердить перечень возможных подходов оценки рисков и на основе этого значительно сузить количество рассматриваемых методов и подходов оценки рисков.

В результате рассмотрения и обобщения действующих, предлагаемых и возможных схем оценки риска ИБ АС, ИТ и организаций можно выделить несколько типовых подходов по решению задач по затрагиваемой проблеме.

1 Первый подход направлен на оценку рисков от реализации предполагаемых угроз с учетом наносимого при этом ущерба. В процессе оценки рисков должны быть рассмотрены все возможные угрозы, вероятности возникновения угроз $P_у$ и последствия реализации угроз в виде определенного ущерба $У_щ$ применительно к конкретной организации или эксплуатируемой ею АС или ИТ. В результате такого рассмотрения для определенного количества угроз, наносящих основной ущерб, (актуальных угроз) принимается решение о необходимости введения барьеров с технической или организационной основой их реализации. При этом остаются угрозы, относительно которых не принято решение о применении защитных мер, и вследствие этого возможен некий ущерб в случае их реализации, что определяет риск. Например, в стандарте ГОСТ Р ИСО/МЭК 15408 данный тип риска определяется как «остаточный риск». Основные этапы первого подхода по оценке риска представлены на рисунке 1.

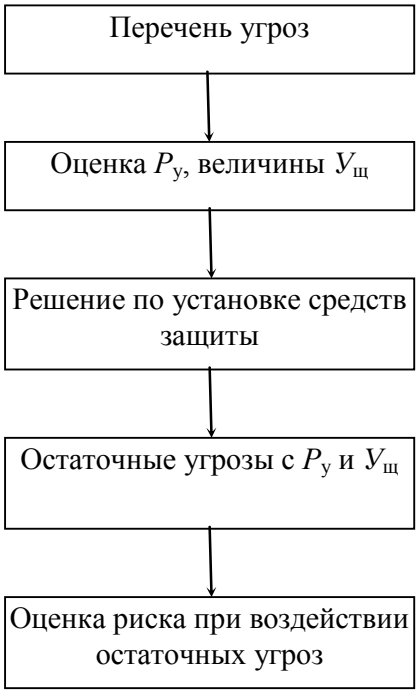


Рисунок 1 - Первый подход оценки рисков

Таким образом, уровень рисков при реализации данного подхода определяется вероятностью возникновения остаточных угроз с учетом остаточных уязвимостей и наносимого при этом ущерба.

Типовыми примерами реализации данного подхода можно считать «Профили угроз OCTAVE» и предложения, изложенные в техническом отчете ISO TR 13569. В данных материалах рекомендуется рассмотрение всех аспектов нарушения основных свойств ИБ – конфиденциальности, целостности и доступности с учетом оценки наносимого ущерба. При этом рассматриваются все последствия раскрытия информации, всех видов ее несанкционированной модификации и отказов по своевременному предоставлению услуг, предположительно с учетом их влияния на бизнес-деятельность организации.

Очевидно, что данный подход весьма трудоемок в реализации, так как требует оценки всех возможных угроз и их последствий, основываясь на полных знаниях исследуемой организации, АС или ИТ, включая, безусловно, знания по всем имеющимся в них уязвимостям. Использование данного подхода позволяет достаточно подробно рассмотреть все аспекты по защите от действующих или известных угроз. Большая трудоемкость использования метода может быть уменьшена за счет реализации подходов, изложенных в техническом отчете ISO/IEC 13335. Рекомендуемые варианты стратегии включают проведение анализа высокого уровня риска для всех систем обеспечения безопасности информационных технологий с тем, чтобы выделить системы с высоким уровнем риска. Затем проводится рассмотрение выделенных систем с использованием детального анализа риска, тогда как к остальным системам может применяться базовый подход (с принятием низкого уровня риска). Применительно к системам с высоким уровнем риска подробное рассмотрение активов, возможных опасностей и уязвимых мест системы будет основой детального анализа риска, что позволит облегчить выбор эффективных мер обеспечения безопасности, соответствующих оцененной степени риска. Использование данного варианта подхода позволит сосредоточить процесс управления риском на областях, отличающихся наивысшим уровнем риска или требующих наибольшего внимания, таким образом может быть разработана программа мер, характеризующаяся наименьшими затратами времени и средств

2 Второй подход направлен на оценку влияния отклонений в конкретных организациях, АС или ИТ от установленного образца, требования к которому закреплены в нормативных документах. При этом предполагается, что при разработке или выборе нормативного документа были рассмотрены все или основные угрозы и их последствия с учетом выработанных политик безопасности в сообществе. Основные этапы второго подхода по оценке риска представлены на рисунке 2.

Таким образом, риск при рассмотрении данного подхода есть оценка степени отклонения от принятых требований ИБ с учетом их важности и влияния на бизнес-деятельность организации.

Типовым примером применения данного подхода можно считать применение в качестве нормативного документа международного стандарта ISO/IEC 17799 и измерение отклонений от требований данного стандарта на основе например использования вопросных модулей продукта «COBRA» для оценки рисков.

Безусловно, данный подход менее трудоемок при его использовании по сравнению с рассмотренным первым подходом, но его применение возможно только в случае разработки такого нормативного документа или принятия какого-либо из известных документов действительно обеспечивающего формирование всех требований, позволяющих при их реализации защититься от всех или основных известных угроз. В связи с использованием оценок на более высоком уровне точность оценки риска будет более низкой, чем при использовании первого подхода.

Рисунок 2 - Второй подход оценки рисков

Однако, во многих случаях, например при проведении работ по сравнению в части степени риска ИБ для различных организаций, но в рамках одной отрасли и занимающихся схожими видами деятельности (реализующих однотипные бизнес-процессы), данный подход может найти широкое применение, что подтверждает практика его широкого применения в международном сообществе. В какой-то мере такой подход может лечь в основу рейтинговых оценок организаций в части обеспечения ими ИБ.

3 Первые два подхода позволяют проводить оценку риска при фиксированном (статическом) состоянии среды, в которой находится объект. Однако, в практической деятельности возникают потребности по необходимости учета влияния на АС, ИТ или организацию факторов динамически изменяющейся внутренней и внешней среды функционирования. Действительно при реальной эксплуатации АС или ИТ ответственность за ИБ переходит от разработчика к эксплуатирующей организации, как правило, с привязкой менеджмента ИБ к общему менеджменту АС, ИТ или организации. При этом, как правило, непрерывно происходят изменения, как в организации и ее среде функционирования, так и технологии, угрозах и других аспектах, что определяет потребности не только в динамическом отслеживании выполнимости требований ИБ, заложенных на этапе разработки, но и оценки влияния всех происходящих динамически изменяемых процессов функционирования на состояние ИБ.

Итак, третий подход ориентирован на оценку рисков ИБ АС, ИТ или организации в условиях реального функционирования в динамически изменяемой среде. Так как оценка выполнимости заложенных при разработке требований ИБ становится недостаточной, то возможный подход может быть направлен на оценку реального состояния организации, АС или ИТ по их функционированию в некоторой устойчивой зоне. Такой подход позволяет определить с достаточно высокой точностью тенденцию к деградации сервисов безопасности, в частности, в направлении резкого ухудшения общего состояния ИБ. Данный подход ориентирован на то, что на основании проведенной разработки и опытного апробирования, например, АС, производится фиксация всех известных и возможных ее показателей, касающихся использования ресурсов, текущей производительности, принятой последовательности выполнения технологических операций, последовательности действий при работе операторов, администраторов и технического персонала и ряда других факторов, и на основании опыта работы

определяются предельные значения параметров, когда работа АС может считаться устойчивой. Данный подход является достаточно новым и по нему имеется незначительная информация в части формирования общей философии организации подходов в части обеспечения ИБ.

Указанный подход базируется на непрерывном мониторинге АС, определении состояния ее параметров и обнаруженных инцидентов ИБ, определении уровня стабильности АС. При выходе параметров функционирования системы за установленные нормы должен формироваться сигнал о переходе АС в состояние повышенного риска (или аномальное состояние), а на основании анализа инцидентов – определение возможных причин, породивших вход АС в эту рисковую зону. Такой подход в технической литературе называется «обнаружение аномалий» – в противовес «обнаружению вторжений». При обнаружении аномалий выявляются и обрабатываются неизвестные событии и таким образом накапливаются знания о динамических изменениях в системе и ее среде. При обнаружении вторжений, как правило, используются имеющиеся знания относительно сценариев возможных вторжений (атак). Оба указанных подхода могут органично дополнять друг друга.

Наличие такой информации позволяет, во-первых, знать о том, что АС в данный момент функционирует в состоянии повышенного риска, а во-вторых, на основе анализа инцидентов и данных систем обнаружения аномалий и вторжений позволяет принимать меры по устранению дефектов, вызванных выявленными инцидентами, и возврату АС в устойчивое состояние. Основные этапы третьего подхода по оценке рисков представлены на рисунке 3.

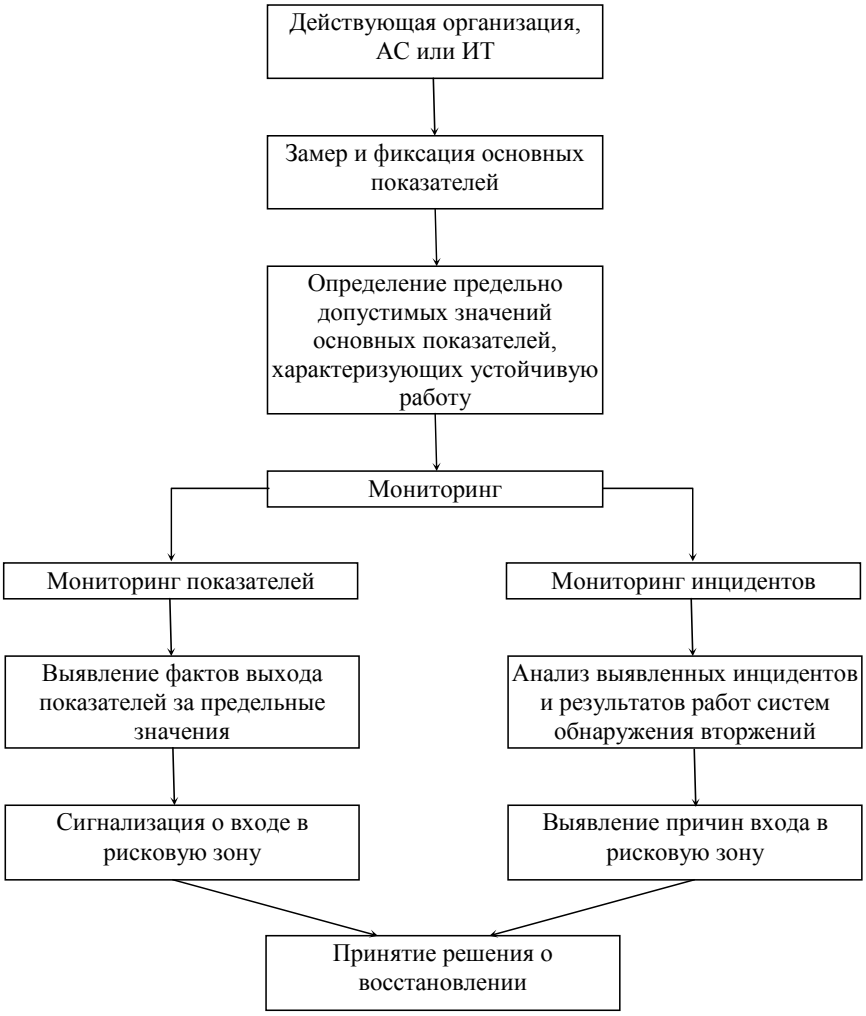


Рисунок 3 - Третий подход оценки рисков

При практической реализации данного подхода будут возникать ограничения, связанные как с невозможностью или сложностью организации мониторинга ряда необходимых параметров АС, так и ограничениями по учету всех различных факторов, способствующих выявлению выхода АС за некоторые предельные значения. Данные отклонения от некоторой идеальной организации мониторинга и будут определять риск, несвоевременности выявления факта входа АС в рисковую зону работы и возможность быстрой деградации ее системы управления ИБ.

Рассматривая возможную область применения данного подхода в общем процессе менеджмента ИБ, следует заметить, что данный подход, ориентируемый на оценку действующих систем, больше лежит в области деятельности подразделений и лиц, непосредственно управляющих или отвечающих за качество их функционирования. Действительно, данный подход связан с мониторингом организации, АС или ИТ, наблюдением за качеством работы как штатных средств защиты, так и изменениями среды функционирования.

Любое отклонение как в работе штатных средств защиты или отклонение среды функционирования от состояния, планируемого на стадии разработки, может привести организацию или систему к кризисно-недопустимому положению, что, безусловно, требует принятия незамедлительных мер. При этом окончательные решения по принятию тех или иных мер, вплоть до снижения уровня ИБ или приостановки работы, должно проводиться на основе обеспечения бизнес-деятельности организации. Такой подход по оценке рисков следует рассматривать крайне необходимым процессом при эксплуатации, позволяющим проводить динамическую оценку состояния рисков ИБ для принятия необходимых мер по управлению ИБ через призму обеспечения бизнес-деятельности организации.

4 Обоснованность введения четвертого подхода оценки рисков базируется на ряде публикаций [13,14]. Метод базируется на принципах, заключающихся в том, что на этапе разработки известны все источники опасностей и их основные характеристики. Например, для оценки защищенности системы от опасных программно-технических воздействий для угроз, порожденных случайными и преднамеренными источниками, определяется частота их воздействия и среднее время воздействия. Считается, что при работоспособности всех заложенных средств зашиты, систему можно считать полностью защищенной, а незащищенность порождается только некачественной работой средств защиты. Для достижения требуемой степени защищенности определяется необходимая частота и глубина диагностических проверок. Снижая время между диагностиками до определенного значения можно добиться определенных величин вероятности работоспособности средств защиты, а, следовательно, и норм обеспечения безопасности. В качестве норм обеспечения безопасности принята вероятность безопасного состояния, определяемая следующими значениями:

– 0,95 при повышенном риске заказчика;

– 0,99 при допустимом риске заказчика.

В качестве примера приведем ряд требований. Например, применяемые технологии защиты от программно-технических воздействий должны обеспечить безопасность функционирования системы в течение суток непрерывной работы:

– с вероятностью $P \geq 0{,}95$ при угрозах от случайных источников, возникающих по статистическим данным не чаще одного раза в неделю, с определенной длительностью интервала;

– с вероятностью $P \geq 0{,}9$ при преднамеренных угрозах, по статистическим данным возникающих с частотой один раз в сутки, также с определенной по статистике длительностью интервала.

При реализации требований РД Гостехкомиссии по классу 3А и 1Б для системы защиты от НСД, системы характеризуются статистическими данными, содержащими:

– среднее время преодоления нарушителем подсистемы идентификации проверки подлинности и контроля доступа;

– среднее время преодоления криптографической подсистемы;

– среднее время защищенности межсетевого экрана.

Основные этапы четвертого подхода по оценке риска представлены на рисунке 4.

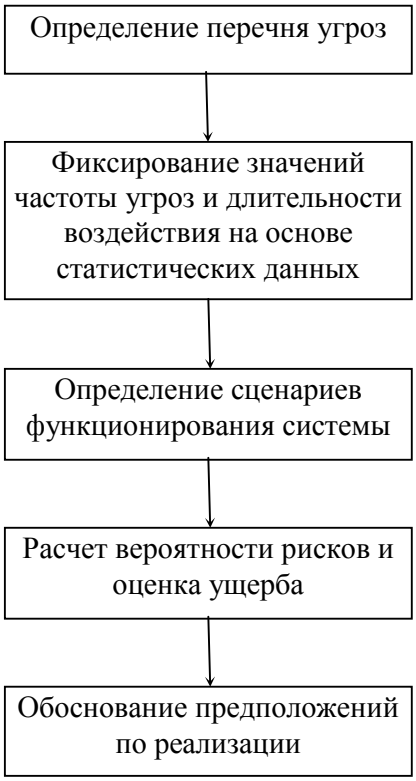


Рисунок 4 - Четвертый подход оценки рисков

Данный подход по оценке рисков по своему сценарию близок как к первому, так и второму подходу. К первому подходу его приближает процесс оценки, начиная с перечня угроз, а ко второму – наличие требований по РД, которые можно считать образцом. Основным отличием подхода является ориентация на существующую статистику появления угроз. Метод более ориентирован не на поиск оптимальных путей обеспечения информационной безопасности, а на оценку выполнения существующих общих требований по защите, определенных действующими документами, и расчете значений риска в виде вероятности нахождения системы в безопасном состоянии, которая определяется в пределах $0{,}95 \leq P_P \leq 0{,}99$ и в полной мере ориентирован на оценку надежности работы с учетом факторов, связанных с ИБ.

Данный подход применим в условиях возможностей определения всего перечня угроз, точных значений по вероятностям их появления и интервалу воздействия, а так же уверенности в том, что защита от выбранного перечня угроз гарантирует требуемый уровень информационной безопасности.

ЗАКЛЮЧЕНИЕ

1. В мировой практике к настоящему времени широкое распространение нашли различные принципы, методы и способы оценки рисков.
2. Как правило, процессы оценки риска ориентированы на использование официально принятых в сообществе, отрасли или государстве нормативных документов.
3. Применение того или иного подхода по оценке рисков ИБ во многом определяется конкретными целями оценки, назначением оценки и использованием результатов оценки.
4. Предложенная в статье классификация подходов по оценке рисков должна оказать методологическую помощь при решении практических задач по оценке рисков ИБ.

ЛИТЕРАТУРА:

1 ISO TR 13569 Банковские и связанные с ними финансовые услуги. Руководство по информационной безопасности. (Banking and related financial services – Information security guidelines).

2 ISO/IEC TR 13335 Информационная технология. Методы безопасности. Руководство по управлению безопасностью (Information technology – Guidelines for the management of IT Security) .

3 ISO/IEC 17799 Information technology – Code of practice for information security management.

4 BS 7799–2-2002 Information security management. Specification with guidance for use.

5 Control Objectives for Information and related Technology (COBIT) 3rd Edition, July 2000.

6 OCTAVE Система Операционной Оценки Критических Угроз, Активов и Уязвимостей, Software Engineering Institute, Carnegie Mellon University.

7 Банковская комиссия Франции, Белая книга «О безопасности информационных систем кредитных учреждений», Январь 1995 г.

8 Basel Committee on Banking Supervision Risk Management Principle for Electronic Banking, May 2001.

9 COBRA. Consultants products, Copyright, 1995–2002, http://www.pcorpu.net.com/cob304exe.

10 UK Government Risk Analysis and Management Method, CRAMM.

11 Uniform Interagency Rating System for Information Technology. URSIT.

12 ГОСТ Р ИСО/МЭК 15408–2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

13 Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Академия АйТи, ДМК Пресс, 2004. – 384 с.

14 Симонов С.В. Анализ рисков, управление рисками. Информационный бюллетень «Jet Info» № 1(68), Москва, 1999.

15 Костогрызлов А.И., Петухов А.В., Щербина А.М. Основы оценки, обеспечения и повышения качества выходной информации в АСУ организационного типа.– М. Изд. «Вооружение. Политика. Конверсия»,1994. – 278 с.

16 Бескоровайный М.М., Костогрызлов А,И., Львов В.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем «КОК». – М.: Изд. «Вооружение. Политика. Конверсия», 2000. – 113 с.

Получено 06.09.2004. Опубликовано в Internet 20.10.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.49-53. Секция-7: Аудит информационной безопасности
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/011)

СПОСОБЫ ДОСТУПА К НАБОРАМ ДАННЫХ ПОДСИСТЕМЫ z/OS RACF

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

Для выполнения автоматизированного анализа данных механизмов протоколирования и аудита среды z/OS необходимо решить проблему переноса этих данных в среду консоли управления аудитора. Очевидно, что в качестве транспортной среды для такого переноса должен выступать компонент операционной системы, поддерживаемый как в ОС z/OS, так и в среде консоли управления, которая реализуется обычно на одной из версий ОС Windows. Таким компонентом является стек протоколов TCP/IP, являющийся частью как одной (z/OS Communication Server), так и другой (Windows Socket, WinSock) операционной системы.

Подсистема контроля доступа к ресурсам ОС z/OS RACF (Resource Access Control Facility), обладает рядом механизмов позволяющих получить данные о состоянии безопасности подконтрольного объекта.

Компонент RACF **IRRADU00** позволяет создавать отфильтрованные выгруженные последовательные (flat) наборы данных, содержащие только типы записей SMF, относящиеся к RACF (SMF80,81,83) и запуску/останову заданий (SMF30), представляющие собой журнал событий RACF. При большом количестве разноформатных данных, фиксируемых SMF по умолчанию, такой вариант наиболее актуален для организации анализа данных, поскольку все записи в журналах RACF относятся непосредственно к событиям, связанным с состоянием безопасности системы и имеют единый фиксированный формат. Формат хранения информации в наборах данных, созданных IRRADU00, адаптирован для последующей загрузки данных SQL-базы данных.

Для анализа системой контроля ресурсов целесообразно выбрать некоторое подмножество типов событий, разделенное на несколько функциональных групп. События следует выбирать исходя из степени их показательности для оценки состояния безопасности и приемлемости для визуальной интерпретации аудитором. Примерный перечень групп и событий приведен в табл. 1.

Таблица 1 – Группы событий журналов регистрации подсистемы RACF

Группа событий	Событие	Обозначение события
Управление ресурсами	Доступ к ресурсу	SMF_ACCESS
	Удаление ресурса	SMF_DELRES
	Определение ресурса	SMF_DEFINE
	Управление списками доступа	SMF_PERMIT
	Изменение общего профиля ресурса	SMF_RALTER
	Переопределение общего профиля ресурса	SMF_RDEFINE
	Удаление общего профиля ресурса	SMF_RDELETE
	Установка режимов использования ресурсов	SMF_SETROPTS
	Добавление тома	SMF_ADDVOL

Группа событий	Событие	Обозначение события
	Удаление тома	SMF_DELVOL
Управление наборами данных	Изменение уровней доступа к наборам данных	SMF_DSAF
	Переименование набора данных	SMF_RENAMEDS
	Добавление набора данных	SMF_ADDSD
	Изменение режимов доступа к наборам данных	SMF_ALTDSD
	Удаление набора данных	SMF_DELDSD
Управление заданиями	Инициализация/завершение задания	SMF_JOBINIT
	Инициализация процесса USS	SMF_INITOEDP
	Завершение процесса USS	SMF_TERMOEDP
Управление пользователями	Добавление пользователя	SMF_ADDUSER
	Модификация пользователя	SMF_ALTUSER
	Присоединение пользователя к группе	SMF_CONNECT
	Удаление пользователя	SMF_DELUSER
	Изменение пароля пользователя	SMF_PASSWORD
	Удаление пользователя из группы	SMF_REMOVE
Управление группами	Удаление группы	SMF_DELGROUP
	Добавление группы	SMF_ADDGROUP
	Модификация группы	SMF_ALTGROUP
Общие операции	Инициализация подсистемы безопасности	SMF_RACFINIT
	Управление подсистемой безопасности	SMF_RVARY
	Формирование общей записи аудита	SMF_GENERAL

Другой компонент RACF **IRRDBU00** позволяет выгрузить базу данных (профили и описания) RACF в последовательный (flat) набор данных для последующей обработки и анализа.

База данных (объектов) RACF содержит в себе подробные профили и описания следующих типов объектов[2]:

1) группы пользователей (Group Data);
2) пользователи (User Data);
3) наборы данных (Data Set Data);
4) общие ресурсы (General Resource Data)

Объект любого типа описывается совокупностью свойств, представляющей собой набор записей (таблиц). Ряд записей носят описательный характер (имена, время создания/модификации и проч.), другие представляют собой формализованное описание политики безопасности для объекта (условия доступа, правила аудита и т.п.). В базе данных RACF храниться также статистическая информация о количестве доступов различного типа к ресурсу (чтение, запись, модификация, управление), поэтому анализ выгруженной базы данных RACF может представлять интерес и с точки зрения количественных оценок состояния безопасности объекта.

Оперативные рабочие данные RACF содержатся в наборах данных, недоступных для анализа. Чтобы получить доступ к данным, необходимо предварительно сделать копии оперативных данных в технологические последовательные наборы данных. Выгрузка журналов регистрации

производится, как правило, с помощью стандартной процедуры выгрузки журналов **DUMPXY**, которая модифицируется соответствующим образом. Процесс выгрузки автоматизирован, с помощью функции JES2 по планированию и выполнению команд операционной системы. Выгрузка может производиться по выполнению команды I SMF раз в сутки или по мере необходимости. Например, команда JES2 $**T A,I=10800,T=23.55,'$VS,"I SMF"'**, будет, начиная с полуночи, с периодичностью в три часа производить переключение активного рабочего набора данных SMF. Изменяя значение параметра I, можно при необходимости увеличить или сократить интервал выгрузки.

Примеры всевозможных карт управления заданиями, позволяющими манипулировать данными RACF, содержатся в библиотеке **SYS1.SAMPLIB**. Для того, чтобы производить одновременно и выгрузку базы объектов RACF, процедуру DUMPXY следует дополнить соответствующей картой управления заданием, подобной следующей

```
//UNLOAD EXEC PGM=IRRDBU00,PARM=NOLOCKINPUT
//SYSPRINT DD SYSOUT=*
//INDD1 DD DISP=SHR,DSN=SYS1.RACF.BACK
//OUTDD DD DISP=SHR,DSN=RACF.IRRDBU00
```

В результате выполнения описанных операций будут сформированы последовательные наборы данных, содержащие журнал регистрации событий и базу объектов RACF. Обычно они имеют наименования **RACFGR.RACF.LOG** и **RACFGR.RACF.COPY**, соответственно.

Наборы данных, сформированные IRRADU00 и IRRDBU00, могут быть перенесены в среду консоли управления аудитора и занесены в БД по трем различным алгоритмам.

Поскольку предполагается, что программы переноса данных для анализа не имеют исполняемых модулей в среде подконтрольных объектов, доступ программ переноса к данным аудита может осуществляться только с помощью стандартных сервисов TCP/IP.

Первый алгоритм запроса предполагает использование запроса данных по протоколу FTP. Данные могут быть получены, как вручную с использованием стандартного клиента FTP ОС Windows и последующей загрузкой в БД системы анализа с помощью стандартных средств СУБД Oracle.

Клиент FTP запрашивает из ОС z/OS упомянутые выше наборы данных RACFGR.RACF.*****. Для доступа к ним необходима учетная запись пользователя системы с соответствующими полномочиями. Такая запись может быть создана специально, но целесообразней использовать существующую учетную запись аудитора **RACFAUD1**. Для получения доступа к системе по FTP этот пользователь должен дополнительно получить полномочия по доступу к среде USS:

```
ALTUSER RACFAUD1
  OMVS(
       UID(0)
       HOME('/u')
       PROGRAM('/bin/sh')
      )
```

Права доступа к журналам регистрации аудитор имеет, для доступа к копии базы объектов ему потребуются следующие дополнительные полномочия

```
PERMIT 'RACFGR.COPY.**'
       ID(RACFAUD1)
       ACCESS(READ)
```

Следует отметить, что такой способ доступа к данным предполагает не оперативный, а отложенный, постфакторный анализ данных аудита наиболее

подходящий для проведения расследований различных нетипичных ситуаций. Какие либо манипуляции с выгруженными наборами данных в среде подконтрольного объекта, помимо описанных выше операций, не требуются.

Перспективным решением, существенно облегчающим доступ к данным RACF, является переход к хранению журналов, профилей и описаний RACF в таблицах базы данных Oracle8i, посредством адаптации процедур из библиотеки SYS1.SAMPLIB, реализующих подобный сервис для базы данных IBM DB2. Реализация такого хранения дает возможность получения данных о состоянии безопасности системы посредством SQL-запросов к базе данных через Oracle Listener (по аналогии с получением данных аудита Oracle) и их последующего оперативного разбора и анализа. Реализация этой возможности позволяет рассмотреть еще два алгоритма получения данных RACF:

1) загрузка журналов, профилей и описаний RACF в таблицы локальной базы данных Oracle8i и последующий доступ к ним из среды консоли управления аудитора посредством SQL-запросов к базе данных через Oracle Listener;

2) загрузка журналов, профилей и описаний RACF непосредственно в таблицы базы данных Oracle8i внешней системы анализа данных аудита

Технически, реализация обоих алгоритмов сравнима по затратам, однако в целях удобства доступа и работы с данными, а равно и точки зрения безопасности, второй алгоритм предпочтительней.

Процедуры, позволяющие манипулировать переносом выгруженных данных RACF в БД, содержатся в библиотеке SYS1.SAMPLIB, а также, в библиотеке ORA.RACF.JOBLIB. Необходимая модификация этих процедур в целях обеспечения данными системы анализа, не представляет, особой сложности и не требует больших трудозатрат, без учета, естественно, организационного аспекта такого рода мероприятий.

Автоматизированный периодический перенос выгруженных данных RACF в БД может быть обеспечен с помощью функции JES2 по планированию и выполнению команд операционной системы, аналогично описанному выше для выгрузки самих данных RACF. В этом случае, процедура переноса данных в БД должна быть помещена в библиотеку SYS1.PROCLIB и может вызываться командой JES2 подобной $**T A,I=10800,T=23.55,'$VS,''S <имя процедуры>'''**.

В заключении следует обратить внимание на возможность использования для анализа данных RACF средств безопасности системы управления Tivoli Management Environment (TME, Tivoli Enterprise), которая обычно используется для организации управления системами на базе майнфреймов. TME включает с себя два взаимосвязанных продукта управления безопасностью – Tivoli Security Management (TSM) и Tivoli User Administration (TUA)[3]. Последние версии TME возможно содержат более широкую номенклатуру продуктов управления безопасностью. Оба упомянутых продукта предназначены, прежде всего, и главным образом, для *управления и администрирования* средств безопасности различных операционных систем (UNIX, NT, NetWare, OS/390). Возможности TSM & TUA позволяют выполнять управление пользователями, политиками доступа, политиками аудита, перенаправление сообщений оператору на консоль управления и т.п.

Для реализации такого управления в среде OS/390 (z/OS) дополнительно требуются два продукта из семейства TME 10 Global Enterprise Manager (GEM): TME 10 GEM OS/390 Connection Service и TME 10 GEM User Administration Service, приобретение которых требует дополнительных существенных затрат.

Таким образом, перенос данных RACF в среду система анализа данных аудита через таблицы БД Oracle, представляется наиболее универсальным и

экономичным, для систем анализа данных штатного аудита объектов гетерогенных информационных систем.

ЛИТЕРАТУРА:

1. С. Симонов, П. Колдышев. Обеспечение информационной безопасности в вычислительных комплексах на базе манфреймов. М: Информационный бюллетень JetInfo, №4 (107)/2002.
2. SA22–7682–03 z/OS V1R4.0 Security Server RACF Macros and Interfaces, Fourth Edition, September 2002.
3. SG24–5339–00 The OS/390 Security Server Meets Tivoli: Managing RACF with Tivoli Security Products, December 1998.

Получено 09.09.2004. Опубликовано в Internet 20.10.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.54-58. Секция-8: Конфиденциальность, целостность, доступность.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/012)

УЧЕБНО-ИССЛЕДОВАТЕЛЬСКАЯ МОДЕЛЬ МНОГОМЕРНОГО ТЕХНИЧЕСКОГО КАНАЛА УТЕЧКИ ИНФОРМАЦИИ

Морозов А.А., Кашаев Е.Д.
Пензенский государственный университет

В соответствии с ГОС ВПО по специальности 090106 «Информационная безопасность телекоммуникационных систем» по дисциплине «Технические средства обеспечения информационной безопасности» предусмотрено проведение лабораторных работ, которые направлены на исследование технических каналов утечки конфиденциальной информации (ТКУИ) и средств их перекрытия.

В настоящее время в нашей стране необходимые учебные стенды по данной тематике серийно не выпускаются. Поэтому на кафедре «Информационная безопасность систем и технологий» Пензенского государственного университета ведется разработка комплекса лабораторных работ для исследования ТКУИ.

Модель комплекса лабораторных работ представляет собой совокупность макетов лабораторных стендов, измерительных средств, ПЭВМ и программного обеспечения к ним.

Для создания комплекса лабораторных работ для исследования ТКУИ были разработаны модели ТКУИ и средств их перекрытия. Разработанные модели относятся к классу физических масштабных моделей, в которых моделируемые системы эквивалентны или подобны оригиналу, либо у систем процесс работы такой же, как у оригинала и они имеют ту же физическую природу, но отличаются от оригинала масштабом [1]. Разрабатываемые модели должны быть идентичны реальным процессам, но моделируемые информативные сигналы должны формироваться с учетом наглядности, необходимой в учебном процессе.

Модель многомерного ТКУИ приведена на рисунке 1.

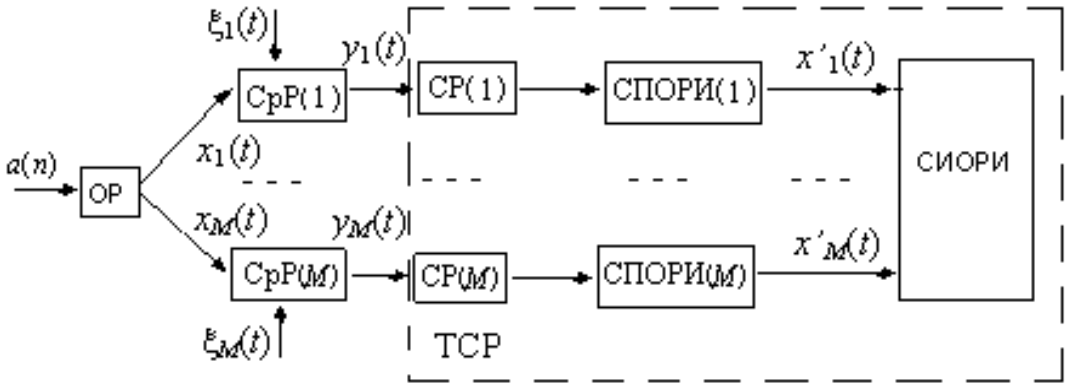


Рисунок 1 - Модель многомерного ТКУИ

На рисунке 1 введены следующие обозначения: ОР – объект разведки; СрР(m) – m-ая среда распространения информативного сигнала; СР(m) – m-ое средство регистрации информативного сигнала; СПОРИ(m) – m-ое средство предварительной обработки результатов измерения; СИОРИ – средство

интегральной обработки результатов измерений; ТСР – технические средства разведки; $n = 1 \ldots N$ – номер внутреннего состояния ОР; $m = 1 \ldots M$ – номер ТКУИ; $a(n)$ – входное n-ое состояние; $x_m(t)$ – информативный сигнал m-го ТКУИ; $x'_m(t)$ – оценка $x_m(t)$; $y_m(t) = x_m(t) * K_m(t) + \xi_m(t)$ – информативный сигнал, поступающий в СР; $K_m(t)$ – коэффициент передачи среды распространения информативного сигнала; $\xi_m(t)$ – объектовая помеха в m-ой среде распространения $x_m(t)$.

Разработанные модели реализованы в виде макетов лабораторных стендов. Макеты позволяют исследовать следующие ТКУИ: по цепям питания, по линейным цепям, по электромагнитным наводкам на соседние цепи и др. Модель технических средств перекрытия каналов утечки информации реализована совокупностью средств, обеспечивающих защиту двумя методами: устранение причин возникновения информативных сигналов и защита от последствий возникновения информативных сигналов.

При организации лабораторных работ по исследованию ТКУИ в качестве ОР рассматриваются лабораторные стенды, проектируемые под конкретные каналы утечки информации. В качестве ТСР используются универсальные измерительные приборы и средства обработки: вольтметры, амперметры, осциллографы, анализаторы спектра, частотомеры и ПЭВМ. В качестве СрР используются цепи питания, цепи заземления, линейные цепи, сигнальные цепи и физические поля. В процессе создания модели были разработаны структурные, функциональные и электрические принципиальные схемы макетов лабораторных стендов, выбраны элементная база, параметры схем, режимы работы макетов, а также разработаны дополнительные схемотехнические решения, обеспечивающие цикловую и тактовую синхронизацию средств измерения и обработки исследуемых сигналов. При разработке учебно-исследовательской модели и ее реализации аппаратно-программными средствами необходимо учитывать следующие факторы и требования: малый уровень информативных сигналов и ограниченные возможности измерительных средств, используемых в учебном процессе; широкий спектр информативных сигналов; сложная объектовая помеховая обстановка во время проведения исследований; необходимость использования в учебных стендах дополнительных органов управления, управляющих и измерительных цепей для обеспечения наглядности.

Одним из направлений исследований процессов утечки информации является ТКУИ по электромагнитным наводкам на соседние и общие цепи [2]. На рисунке 2 приведена структурная схема макета лабораторного стенда для исследования утечки информации по электромагнитным наводкам на соседние цепи.

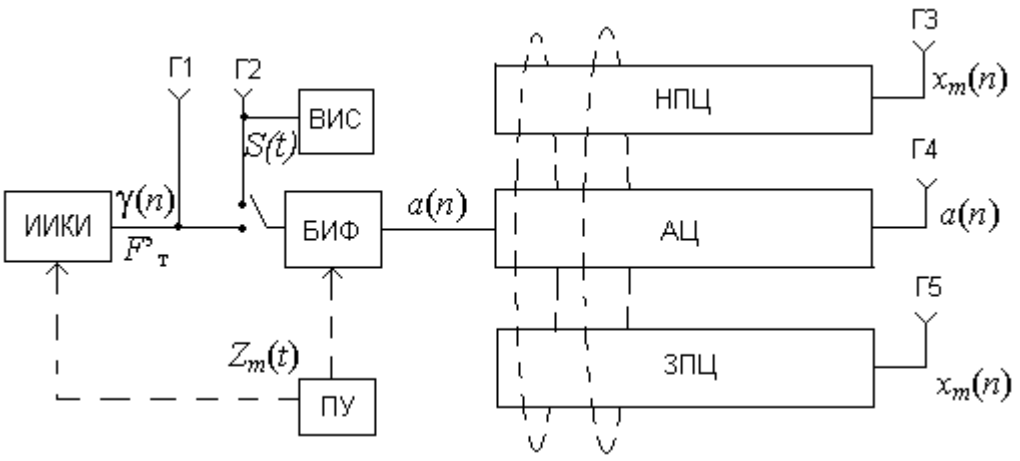


Рисунок 2 – Структурная схема макета

Схема состоит из следующих блоков: ИИКИ – имитатор источника конфиденциальной информации; ВИС – внешний источник сигналов; БИФ – блок изменения фронта импульса; ПУ – пульт управления; НПЦ – блок незащищенных пассивных цепей; АЦ – блок активных цепей; ЗПЦ – блок защищенных пассивных цепей.

Информационный сигнал $a(n)$ может поступать в блок активных цепей от имитатора источника конфиденциальной информации или внешнего источника сигналов. Задающий генератор имитатора источника конфиденциальной информации вырабатывает импульсы с частотой $F_{зг} = 7{,}8$ МГц. В формирователе тактовых частот предусмотрено понижение тактовой частоты с помощью группы делителей до 7,6; 15,2; 30,4 и 60,8 кГц. Тактовые частоты поступают на входы управляемого мультиплексора. С выхода мультиплексора сигнал выбранной тактовой частоты F_T' поступает в управляемую рекуррентную линию задержки для формирования псевдослучайной последовательности (ПСП) $\gamma(n)$. Управляемая рекуррентная линия задержки может формировать ПСП с периодом $T_{ПСП} = 7, 15, 31$ или 63 такта. Запуск управляемой рекуррентной линии задержки, выбор тактовой частоты и периода ПСП осуществляется с пульта управления сигналом $Zm(t)$ во время проведения исследований. Цикловая частота $F_ц$, необходимая для синхронизации развертки лучей осциллографа, вырабатывается в формирователе цикловой частоты из ПСП. Сигнал, поступающий от внешнего источника сигналов, $S(t)$ может иметь различные параметры (форму, амплитуду, частоту, период, длительность). В макете предусмотрено изменение фронтов импульсов информационного сигнала в блоке изменения фронта импульса.

Макет позволяет имитировать утечку информации по электромагнитным наводкам на соседние цепи как внутри аппаратуры, так и в помещении. Для этого имитатор активных и пассивных цепей выполнен в двух вариантах: в металлическом корпусе с возможностью его заземления и в деревянном корпусе.

Параметры макета выбирались таким образом, чтобы обеспечить наглядность исследуемых процессов и возможность фиксирования информативного сигнала имеющимися измерительными приборами. Длина проводов активных и пассивных цепей была выбрана от 20 до 150 см.

В качестве средств защиты от утечки информации по электромагнитным наводкам на соседние цепи в макете используются экраны: сплошной стальной, сплошной медный, медная оплетка, алюминиевая фольга, а также применяется пространственное зашумление.

Макет позволяет студентам при исследовании получать зависимости уровня наведенного сигнала от: частоты сигнала в активной цепи (Uп(Fвнешн)), от расстояния между активной и пассивной линиями (Uп(L)), сопротивления на дальнем конце линии (Uп(Rд)), амплитуды импульсов сигнала в активной цепи (Uп(Uа)), крутизны импульсов сигнала в активной цепи (Uп(τф)).

На рисунках 3, 4, 5 приведены примеры получаемых результатов лабораторных исследований для конкретных вариантов задания.

На рисунке 3 приведены результаты исследования уровня наведенного сигнала в незащищенных и защищенных пассивных цепях макета от частоты сигнала в активной цепи, при постоянных значениях Rд = 4,7 кОм, L = 60 мм, Uа = 3 В. На рисунке обозначено: Uп1 – уровень сигнала в незащищенной пассивной цепи; Uп2 – уровень сигнала в защищенной пассивной цепи (медный экран); Uп3 – уровень сигнала в защищенной пассивной цепи (стальной экран); Uп4 – уровень сигнала в защищенной пассивной цепи (комбинированный экран).

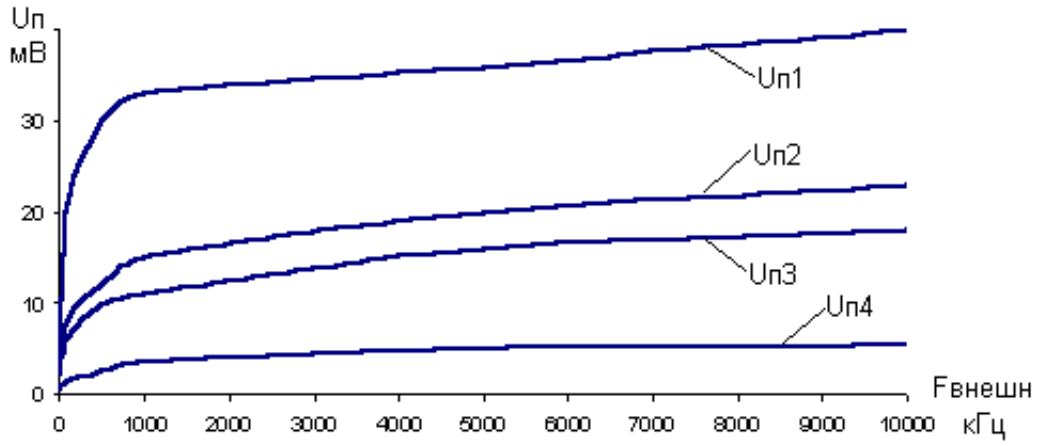


Рисунок 3 – Зависимость уровня наведенного сигнала в пассивной цепи от частоты сигнала в активной цепи

На рисунке 4 приведены результаты исследования уровня наведенного сигнала в незащищенных и защищенных пассивных цепях макета от расстояния между пассивной и активной цепью, при постоянных значениях Rд = 4,7 кОм, Fвнешн = 1 МГц, Uа = 3 В.

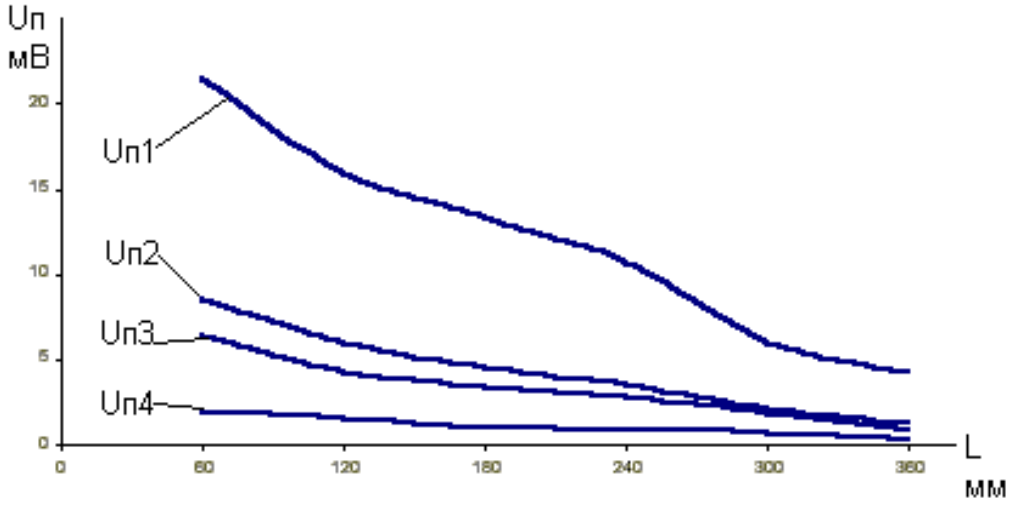


Рисунок 4 – Зависимость уровня наведенного сигнала в пассивной цепи от расстояния между активной и пассивной цепями

В таблице 1 и на рисунке 5 приведены результаты исследования уровня наведенного сигнала в незащищенных пассивных цепях макета от крутизны фронта τф импульсов информационного сигнала в активной цепи, при Fвнешн = 100 кГц, Rд = 4,7 кОм, L = 60 мм, Uа = 3 В, при условии τф1 > τф2 > τф3 > τф4.

Таблица 1

τф	τф1	τф2	τф3	τф4
Uп, мВ	7	13	24	27

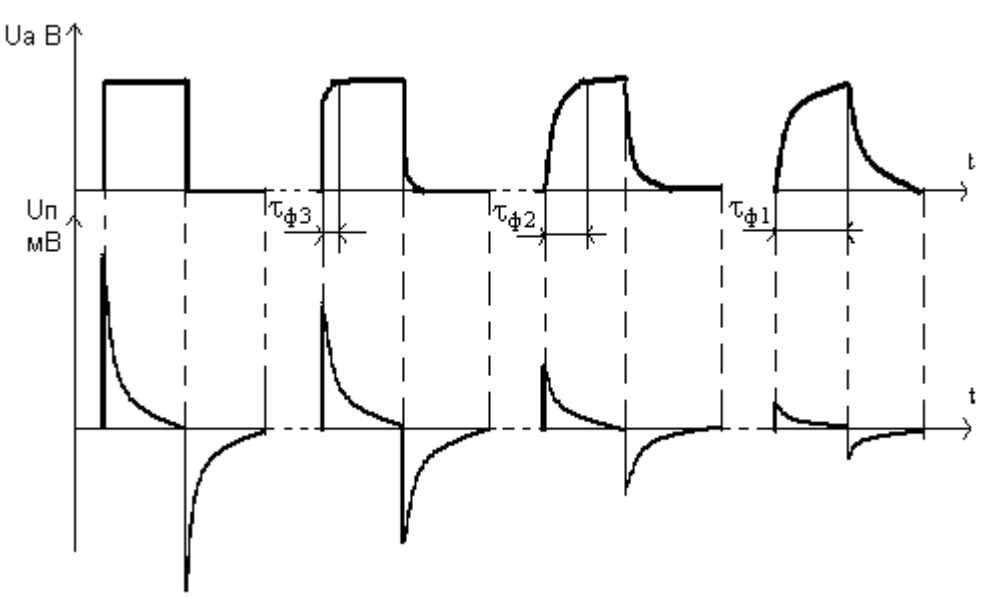


Рисунок 5 – Зависимость уровня наведенного сигнала в пассивной цепи от крутизны фронта импульса информационного сигнала в активной цепи

При выполнении лабораторных работ студенты имеют возможность исследования процедуры маскирования информативного сигнала, например, исследование параметров наведенного сигнала в пассивных цепях при использовании пространственного зашумления. В качестве источника шума могут использоваться различные приборы, например, генератор Г2-57. Студентам предоставляется возможность убедиться, что при уровне шума, превышающим уровень некоторых видов наведенного информативного сигнала в 1,5 и более раз, они становятся визуально неразличимым на фоне шума.

При проведении лабораторных работ студентами исследуются следующие способы уменьшения уровня наводимого информативного сигнала: понижение частоты сигнала в цепях; уменьшение уровня сигнала в цепях; увеличение расстояния между цепями; уменьшение величины сопротивления на дальнем конце линии; увеличение длительности фронтов импульсов сигнала; экранирование; пространственное зашумление.

Результаты экспериментальных исследований разработанной учебно-исследовательской модели показали, что выбранный набор параметров модели, технических решений и режимов работы позволяет студентам старших курсов в процессе обучения убедиться в реальности исследуемых ТКУИ и получить представление об эффективности используемых технических средств защиты информации. Таким образом, разрабатываемые лабораторные стенды позволят выполнить требования ГОС ВПО по специальности 090106.

ЛИТЕРАТУРА:

1. Советов Б.Я., Яковлев С.А. Моделирование систем. – Учебник для вузов по спец. «Автоматизированные системы управления». – М.: «Высш.школа»., 1985. – 271 с.
2. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. М.: Российск.гос.гуманит.ун-т., 2002. – 399 с.

Материалы поступили 24.09.2004. Опубликовано в Internet 20.10.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.59-60. Секция-3: Нормативное, методологическое и методическое обеспечение информационной безопасности.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/013)

УЧЕБНО-ИССЛЕДОВАТЕЛЬСКАЯ МОДЕЛЬ ЗАЩИЩЕННОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ

Кашаев Е.Д. E-mail: kashaev@beda.stup.ac.ru
Пензенский государственный университет

В соответствии с образовательными стандартами на специальности 090105, 090106 учебные планы предусматривают изучение различных методов обработки, передачи, приема и защиты информации в различных дисциплинах. При этом фактически в разных дисциплинах изучаются методы, относящиеся к различным иерархическим уровням автоматизированной системы. При таком подходе у большинства студентов возникают проблемы с восприятием изучаемого материала как единого целого и, соответственно, затрудняется восприятие проблем взаимного увязывания требований, методов передачи и защиты информации и их свойств, технологий управления безопасностью систем передачи данных (СПД) особенно в изменяющихся условиях информационного противоборства.

Для обеспечения восприятия защищенной СПД как единого комплекса, включающего взаимоувязанные процедуры основных и защитных функций системы, необходимо использовать единую учебную модель защищенной СПД, компоненты которой использовались бы при изучении основных и защитных функций в различных дисциплинах. При таком подходе по мере изучения дисциплин появляется возможность идти по пути все более полного использования модели защищенной СПД. Такая методика позволит на пятом курсе обучения в ВУЗе в рамках курсового проектирования нескольких дисциплин одного семестра провести всесторонние исследования защищенной СПД от различных видов атак по отдельности и в совокупности, используя полученные ранее знания и опыт.

Использование единой модели позволит проводить исследования способности различных методов и их сочетаний противодействовать непреднамеренным и преднамеренным скрытным и явным атакам на компоненты СПД. Студенты будут иметь возможность получения набора различных основных изучаемых зависимостей. Среди этих зависимостей могут оказаться такие, которые отражают противоречивый характер предложенных и исследуемых студентом методов с позиций какого-либо требования. Ситуации противоречия чего-либо позволят студентам получать навыки разрешения возникающих противоречий, искать компромиссы между различными требованиями к исследуемой СПД и свойствам предлагаемых защитных процедур для различных условий эксплуатации с позиций общесистемных требований и критериев. Это позволит реально ощутить и глубже понять сложность проблемы проектирования СПД различного класса защищенности и необходимость использования математического аппарата оптимизации принимаемых решений для многопараметрических систем при решении задач большой размерности. Таким образом, у будущего специалиста будет формироваться системный подход к исследованию процессов функционирования СПД в условиях информационного противоборства. Разработка учебной модели противоборства двух автоматизированных систем является сложной задачей, потому что она должна

учитывать декомпозицию систем с учетом деления материала по дисциплинам и по семестрам, а также наращивание возможных функций атакующей и защищаемой систем в процессе обучения.

На кафедре «Информационная безопасность систем и технологий» Пензенского государственного университета» ведется разработка модели защищенной СПД и использование разработанных компонентов модели в учебном процессе и в научных исследованиях. Спецификой разработки программного обеспечения для учебного процесса является сложность разработки интерфейса пользователя, удобного для студентов различных курсов с разным уровнем знаний. Специфика исследования методов защиты информации в учебном процессе заключается в том, чтобы за отведенное время (для лабораторных работ, курсового проектирования) студент мог получить статистические характеристики, позволяющие построить требуемые зависимости. Для этого предлагается использовать алгоритмы, рекомендуемые различными ГОСТами в упрощенном виде. Например, изменяя длину имитовставки в криптоалгоритме по ГОСТ 28147–89 в сторону уменьшения, увеличивая вероятности проведения преднамеренных и непреднамеренных атак.

Разработанные к настоящему времени компоненты модели канального уровня позволяют исследовать методы защиты информации от непреднамеренных атак (помех) на основе введения избыточности различного вида, в частности, помехоустойчивое кодирование с обнаружением и исправлением ошибок, многократная передача кодовых слов, обратная связь. Модель дискретного источника помех позволяет задавать вероятность появления ошибок в дискретном канале, законы распределения пачек ошибок.

Разработанные компоненты модели физического уровня позволяют задавать статические и динамические характеристики следующих каналов связи: канала тональной частоты, КВ-канала, гидроакустического канала и их комбинаций. Разработана модель аналогового источника помех и преднамеренных атак как на аналоговый сигнал в канале связи, так и на частотно-временные характеристики канала связи. Разработана модель устройств преобразования сигналов.

В плане развития модели защищенной СПД ведется разработка следующих компонентов: источника дискретной информации; источника аналоговой, в том числе речевой информации; речепреобразующих устройств; вокодеров; липредеров; аналогово-цифровых маскираторов речи; средств криптографической защиты данных, обеспечивающих конфиденциальность, целостность и подлинность. Все компоненты модели могут быть использованы в любом приемлемом сочетании, например, аналоговый источник речи, одна из процедур преобразования речи, дискретный канал связи. Разработка учебной модели физического и канального уровня может служить основой для дальнейшего развития моделей сетевого и транспортного уровней защищенной СПД.

Таким образом, разработка и использование предлагаемой единой учебно-исследовательской модели защищенной системы передачи данных в различных дисциплинах позволит повысить качество подготовки специалистов в области проектирования и эксплуатации защищенных систем связи и управления.

Материалы поступили 24.09.2004. Опубликовано в Internet 20.10.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.61-63. Секция-5: Управление информационной безопасностью.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/014)

ВЛИЯНИЕ ПОГРЕШНОСТИ ФАЗОВОЙ СИНХРОНИЗАЦИИ БАЗИСНЫХ ФУНКЦИЙ НА ТОЧНОСТЬ ТЕКУЩЕЙ ОЦЕНКИ ОТНОШЕНИЯ СИГНАЛ/ШУМ

Егорова Н.А. E-mail: egorova@beda.stup.ac.ru
Пензенский государственный университет

Одной из задач подсистемы информационной безопасности автоматизированных систем декаметровой радиосвязи является оценка помеховой обстановки в отведенном диапазоне радиочастот, которая решается с помощью сканирующего радиоприемника. Однако данный метод сканирования не позволяет оценить в точке приема отношение сигнал/шум h во время сеанса связи.

В [1] был предложен метод оперативной оценки отношения h в быстроменяющейся помеховой обстановке в процессе передачи сообщения. Этот метод рассчитан на работу при значениях $h > 2$, характерных для нормальной помеховой обстановки. Однако при организации связи с подвижными объектами в быстроменяющейся сложной помеховой обстановке возникает необходимость оперативного обнаружения ситуаций, когда отношений h в процессе передачи стало меньше допустимой величины на заданной скорости для конкретной системы передачи данных. При использовании для защиты от помех методов синхронного накопления и/или помехоустойчивого кодирования допустимая величина h на скоростях передачи данных от 50 до 1200 бит/с может быть меньше единицы.

Для оперативной оценки текущих значений отношения сигнал/шум при условии $h < 2$ предлагается использовать спектрально-временной способ цифровой обработки сигналов. Если наложить условие, что для оперативной оценки значения $h(t)$ приемлема некая погрешность, то вычисления значения $h(t)$ можно делать на конечном временном интервале. С учетом указанных условий была предложена методика вычисления $V(j)$ на основе вычисления энергии помехи без учета спектральной составляющей, совпадающей с несущей частотой.

Процедура вычисления оценки $V(j)$ на j-ом временном интервале анализа заключается в следующем. Сначала выбирается размер дискретного базиса N и вычисляется длина интервала анализа $T = NT_д$, где $T_д$ – период дискретизации. Интервал анализа T может находиться в пределах от единиц до нескольких сотен длительностей посылок в зависимости от требований к оперативности, точности и вычислительной сложности проведения оценки.

Затем формируется тригонометрический базис $\boldsymbol{F}(j)$, в который должна входить базисная функция, совпадающая с несущей частотой информационного сигнала на интервале ортогональности (анализа) T. Так как в реальных каналах связи присутствует рассинхронизация несущих частот устройств преобразования сигналов (УПС), то необходимо ввести процедуру синхронизации и фазирования базиса с несущей частотой на каждом j-ом интервале на основе известных алгоритмов, применяемых в УПС.

Далее осуществляется скачущее j-ое прямое дискретное ортогональное преобразование в соответствии с выражением

$$\boldsymbol{A}(j) = \boldsymbol{F}(j)\boldsymbol{S}(j),$$

где $\boldsymbol{S}(j)$ – матрица-строка принятой из канала связи смеси информационного сигнала и шума.

Для исключения спектральных составляющих, совпадающих с несущими частотами, выполняется следующее преобразование

$$\boldsymbol{A}_{\mathrm{c}}(j) = \boldsymbol{H}\boldsymbol{A}(j),$$

где $\boldsymbol{H}$ – диагональная единичная матрица, в которой значение диагональных элементов, умножаемых на коэффициенты из матрицы $\boldsymbol{A}(j)$, соответствующие несущей частоте, равны нулю.

Синтезированный шум $\xi_{\mathrm{c}}(j)$ формируется в процессе обратного дискретного ортогонального преобразования в соответствии с выражением

$$\xi_{\mathrm{c}}(j) = \boldsymbol{F}^{-1}(j)\boldsymbol{A}_{\mathrm{c}}(j).$$

Для каждого j-ого интервала оценки определяется уровень синтезированного шума U_{c} и вычисляется текущая оценка $V(j)$

$$V(j) = \frac{U_x(j)}{U_{\mathrm{c}}(j)},$$

где U_x – уровень информационного сигнала.

Для проверки работоспособности предложенного способа были проведены экспериментальные исследования на основе разработанной имитационной модели. Точность определения уровня помехи оценивалась по относительной погрешности δ, вычисляемой по формуле

$$\delta = \frac{U_{\xi}(j) - U_{\mathrm{c}}(j)}{U_{\xi}(j)}.$$

На рисунке 1 приведены зависимости относительной погрешности δ от отношения h в канале связи при различном размере базиса N для условий использования относительной фазовой модуляции сигналов и скорости передачи данных 600 бит/с.

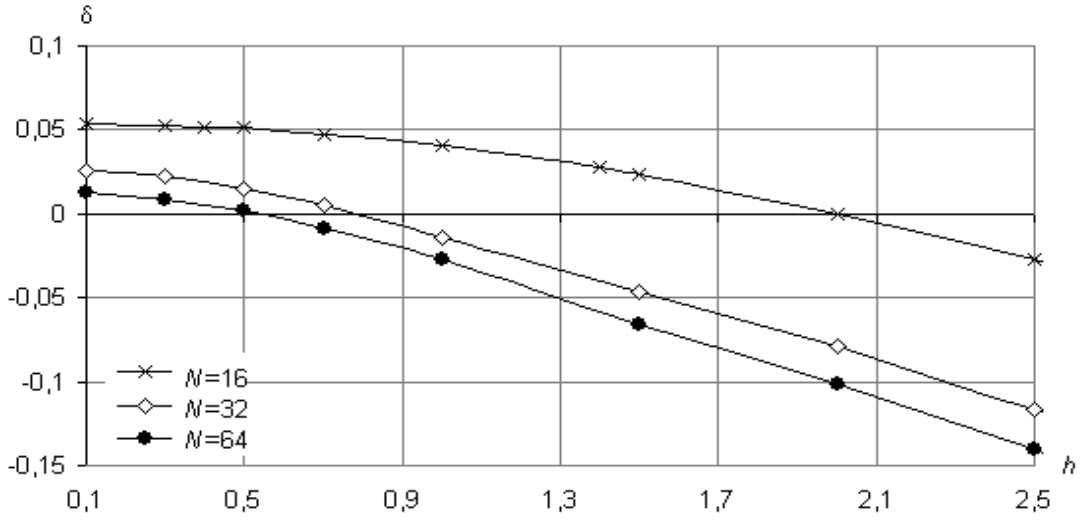


Рисунок 1 - Зависимость погрешности δ от отношения h при различном размере базиса N для скорости 600 бит/с

На рисунке 2 приведены зависимости относительной погрешности δ от отношения h в канале связи при различной скорости передачи данных для условий использования относительной фазовой модуляции сигналов и размера базиса N=64 отсчета частоты дискретизации.

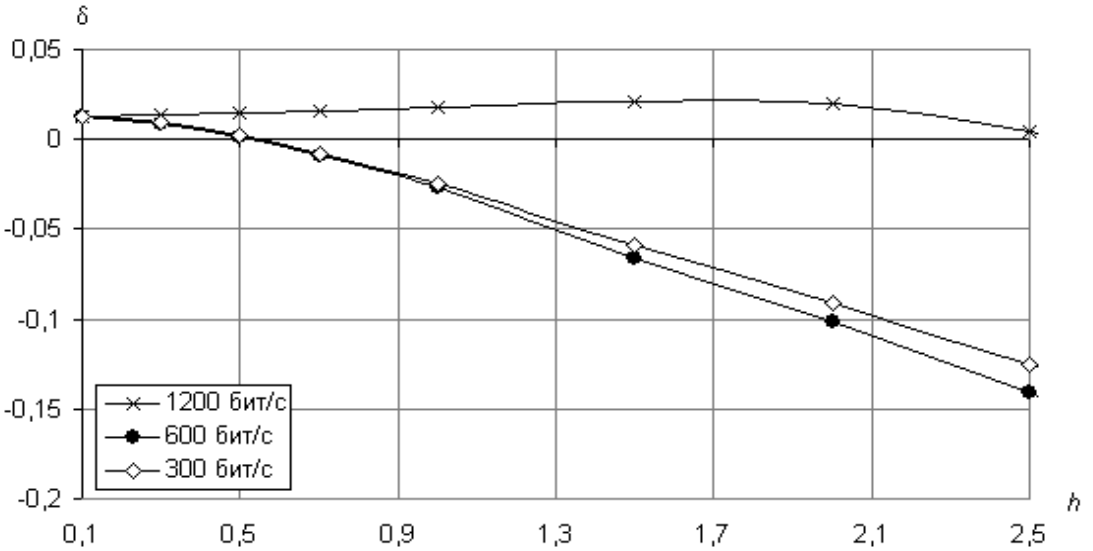


Рисунок 2 - Зависимость погрешности δ от отношения h при различной скорости C для размера базиса N =64

На рисунке 3 приведены зависимости относительной погрешности δ от величины расфазирования базиса относительно несущей частоты $\Delta\varphi$ при различной скорости передачи данных для условий использования относительной фазовой модуляции сигналов и размера базиса N=32 отсчета частоты дискретизации. Кривые получены для значений отношения сигнал/шум в канале связи h=1,5 и h=0,7.

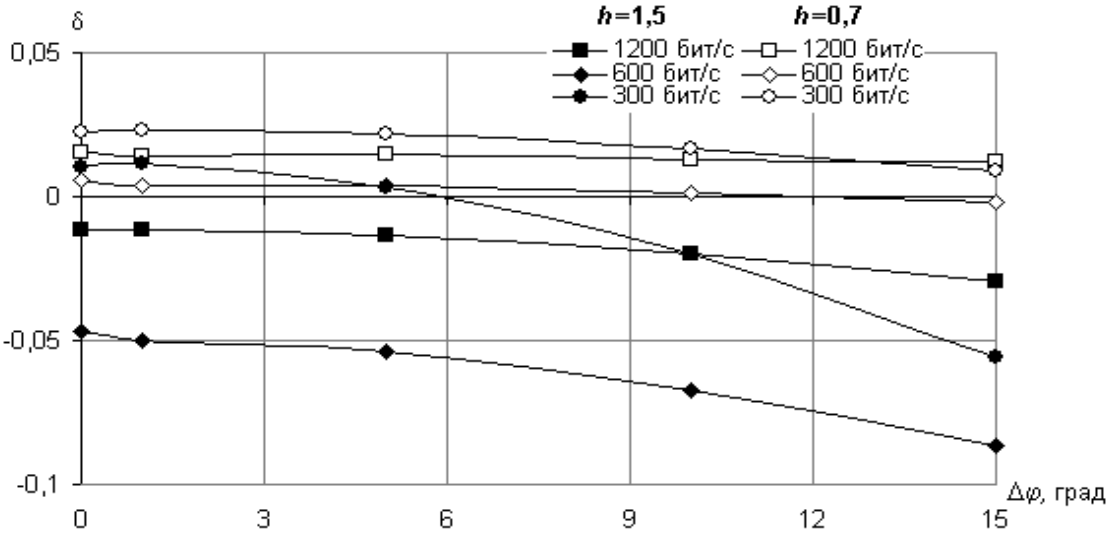


Рисунок 3 - Зависимость погрешности δ от величины расфазирования $\Delta\varphi$ базиса относительно несущей частоты

По результатам проведенных исследований можно сделать следующие выводы: для значений $h < 2$ относительная погрешность δ находится в интервале [– 0,05; 0,05] и мало зависит от размера базиса N; до величины $\Delta\varphi$=5° значение погрешности δ изменяется мало.

ЛИТЕРАТУРА:

1. Кашаев Е.Д., Гридасов В.Г. Экспресс-анализ помеховой обстановки в канале связи. Деп. в ВИНИТИ 31.03.00, №869-В00.

Материалы поступили 24.09.2004. Опубликовано в Internet 20.10.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.64-67. Секция-6: Системы обнаружения вторжений.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/015)

ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ ДЛЯ РЕШЕНИЯ ЗАДАЧ МОДЕЛИРОВАНИЯ И КЛАССИФИКАЦИИ СЕЙСМИЧЕСКИХ СИГНАЛОВ НАРУШИТЕЛЕЙ В НЕЙРОСЕТЕВОМ БАЗИСЕ

Дудкин В.А., Захаров С.М., Акимова Ю.С.
Пензенский государственный университет
Кафедра: «Автономные информационные и управляющие системы»

Современный уровень разработки интеллектуальных информационных систем, к которым относится система обнаружения и классификации объектов связан с компьютерным моделированием. Любая модель требует подтверждения адекватности реальным процессам на достаточно большом объеме данных. Как двадцать лет назад, так и в настоящее время существуют определенные трудности в создании банка записей сейсмических сигналов объектов.

Перспективным направлением в настоящее время также является построение классификаторов на базе нейронных сетей.

Для решения двух поставленных задач разработан интерфейс "*Seysmoneyro*". Он позволяет моделировать сейсмические сигналы сейсмофона, одного человека и группы людей (3 и более человек); формировать, обучать и тестировать нейронную сеть для задач обнаружения полезного сигнала и классификации его по классам «Один человек» – «Группа людей».

Интерфейс моделирует работу пьезоэлектрического акселерометра. При синтезе сигналов принято допущение о том, что грунт является изотропной упругой средой, а скорость распространения колебаний во всех направлениях одинакова. Изменяемыми параметрами являются характеристики грунта, скорость и трасса движения, длина шага и масса человека, количество людей в группе.

Работа интерфейса состоит из нескольких этапов. Рассмотрим их на примере задачи обнаружения.

На первом этапе создаются два класса: Класс 1 – полезный сигнал (один человек или группа людей) (рисунки 1 и 2) и Класс 2 – сейсмофон (рисунок 3).

На втором этапе формируется структура нейронной сети и настраиваются коэффициенты синаптической карты. В интерфейсе запрограммирована однослойная радиальная базисная сеть и используется алгоритм быстрого обучения. Количество входов нейронной сети равно размерности вектора входных данных, выход один. Используется пороговая функция активации.

За показатель качества обучения нейросетевого классификатора выбран параметр q, который вычисляется по выражению [1]:

$$q = \frac{|m_1 - m_2|}{d_1 + d_2},$$

где m_1, m_2 и d_1, d_2 – оценки математического ожидания и средних квадратических отклонений по классам 1 и 2 соответственно (рисунок 4). Теоретически параметр q может изменяться от нуля до бесконечности. Реально его значение не превышает 10 – 15 единиц.

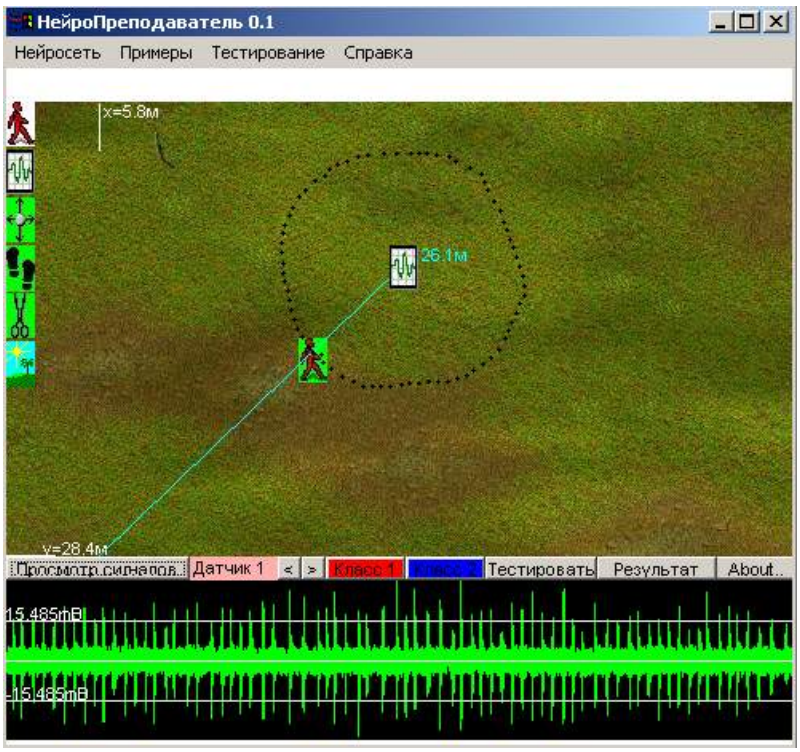


Рисунок 1 – Сейсмический сигнал одного человека

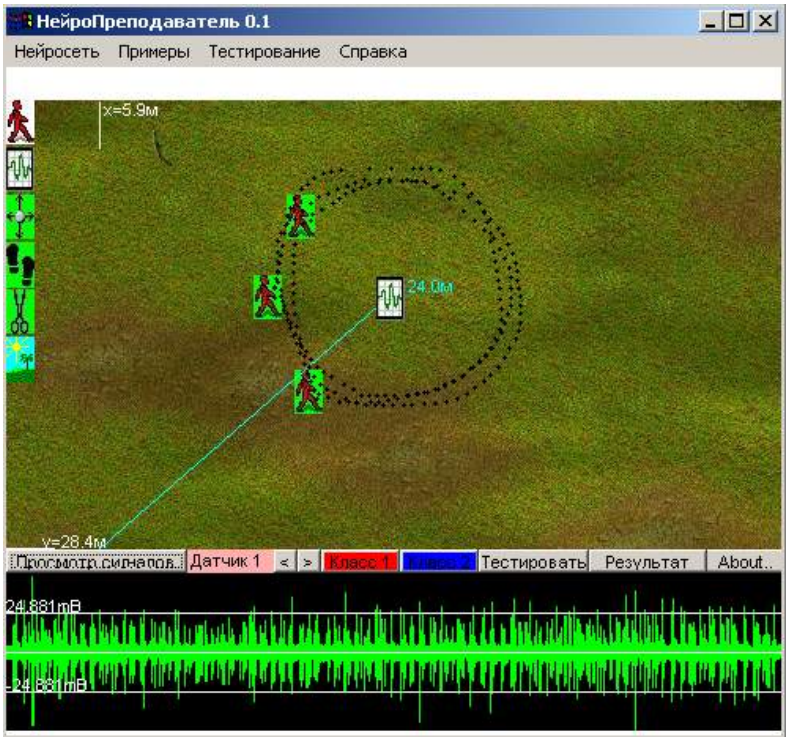


Рисунок 2 – Сейсмический сигнал группы людей

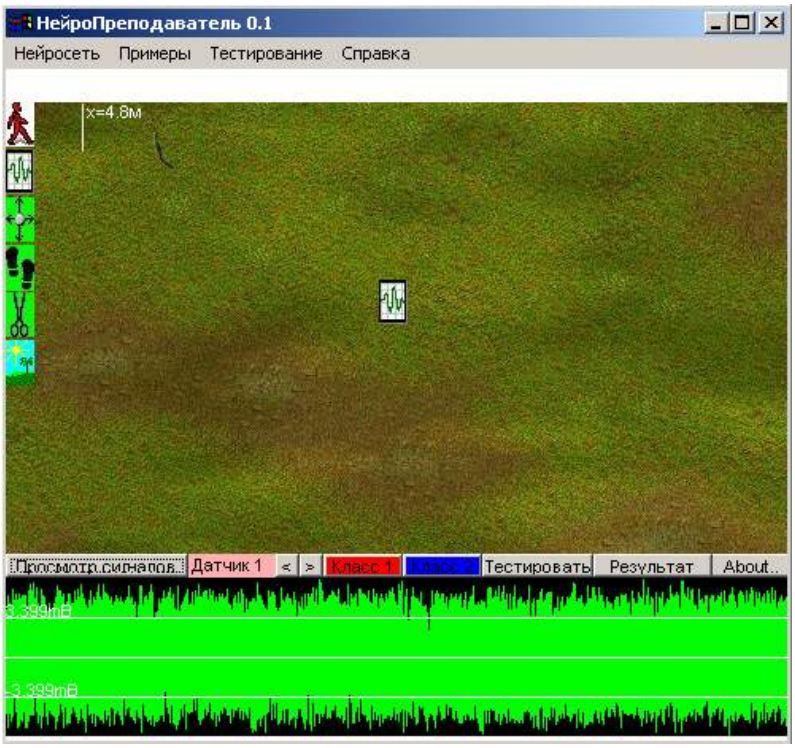


Рисунок 3 – Сигнал сейсмофона

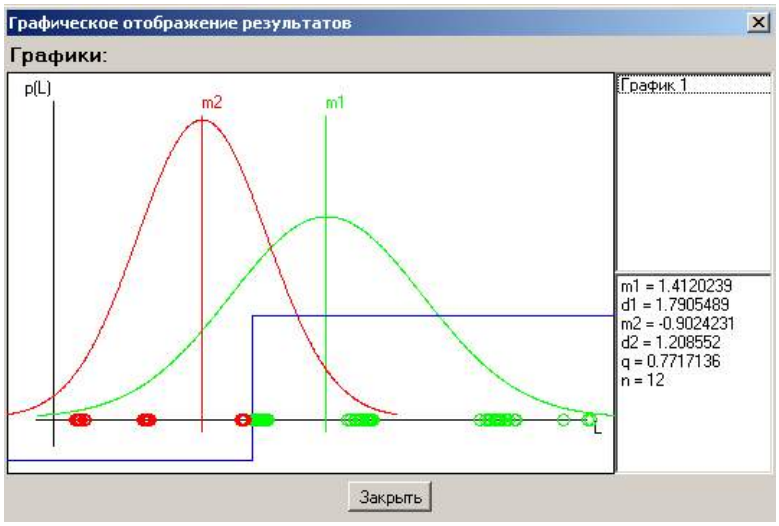


Рисунок 4 – Два класса сигналов с выхода нейронной сети после первого обучения

Экспериментально установлено, что нейросетевой классификатор обеспечивает вероятность правильного обнаружения не менее 0.95 при расстоянии до сейсмического приемника 30 м и вероятность правильной классификации не менее 0.85 на траверзе до 15 м при значении параметра качества не менее единицы ($q \geq 1$).

Если оценки показателей эффективности нейросетевого обнаружителя ниже требуемых, необходимо поднять нижний порог качества и заново обучить нейронную сеть (рисунок 5). При этом автоматически исключаются неинформативные признаки и значение параметра q возрастает.

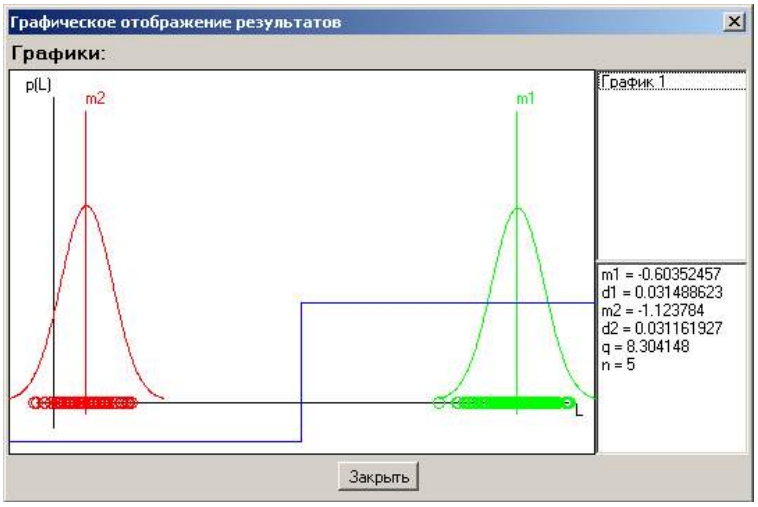


Рисунок 5 – Результаты переобучения нейронной сети

Если после переобучения нейронной сети, не удается добиться повышения качества ее работы, необходимо заново сформировать обучающие множества первого и второго классов и попробовать на них обучить нейронную сеть.

На третьем этапе проводится тестирование работы нейросетевого обнаружителя. Для оценки вероятности правильного обнаружения необходимо сгенерировать сейсмический сигнал одного человека и протестировать на нем работу нейронной сети. При этом сигнал окрашивается в цвет, соответствующий одному из классов. Оценки вероятности правильного обнаружения и пропуска человека вычисляются автоматически.

Для оценки вероятности ложной тревоги генерируется сигнал сейсмофона и проводится тестирование нейронной сети.

Результаты тестирования работы нейросетевого классификатора позволяют сделать вывод о том, что с вероятностью не менее 0.95 можно обнаружить человека в зоне радиусом 10 м от сейсмоприемника. При этом оценка вероятности ложной тревоги не превышает 0.02.

В задаче классификации все этапы работы повторяются. Разница лишь в том, что в Класс 1 записываются сигналы одного человека (рисунок 1), а в Класс 2 – группы людей (рисунок 2). Тестирование работы классификатора дали оценки вероятности правильной классификации не менее 0.9 в той же зоне чувствительности.

В дальнейшем планируется улучшить работу интерфейса за счет количественного и качественного изменения пространства входных признаков и увеличения числа слоев нейронной сети. Количество признаков может доходить до 100. Планируется дополнить интерфейс модельными сигналами техники.

ЛИТЕРАТУРА:

1. Волчихин В.И., Иванов А.И. Основы обучения искусственных нейронных сетей. Пенза – 2004, Издательство пензенского государственного университета, 116 с.

Материалы поступили 29.10.2004. Опубликовано в Internet 20.12.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С. 68-70. Секция-6: Системы обнаружения вторжений.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/016)

ИСПОЛЬЗОВАНИЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ ДЛЯ ЭФФЕКТИВНОЙ ФИЛЬТРАЦИИ СЕЙСМИЧЕСКИХ СИГНАЛОВ ИДУЩИХ НАРУШИТЕЛЕЙ

Дудкин В.А. Вольсков А.А. E-mail: cirix@penza.net
Пензенский государственный университет

При обработке сильно зашумленных сигналов традиционной процедурой является их частотная фильтрация. Реализуется такая процедура использованием частотных фильтров, полоса пропускания которых согласовывается с эффективной полосой частот принимаемых полезных сигналов. Частотные фильтры повышают отношение сигнал/шум на своем выходе тем больше, чем меньше отношение эффективной полосы полезного сигнала к общей ширине спектра зашумленного сигнала. Основным недостатком использования частотных фильтров является невозможность удаления шумовой составляющей из эффективной полосы полезного сигнала. Сейсмические сигналы от идущих в зоне обнаружения нарушителей относятся к классу сильно зашумленных сигналов. Поэтому проблема выделения их на фоне сейсмошумов является весьма актуальной. Недостатки традиционного метода частотной фильтрации обусловили необходимость использования для обработки сейсмических сигналов более эффективных методов фильтрации. К таким методам в настоящее время можно отнести вейвлет-фильтрацию.

Для сравнительной оценки методов воспользуемся сейсмическими сигналами, смоделированными с помощью программы «Интерфейс» [1]. На рисунке 1 а) показан исходный сейсмический сигнал группы нарушителей из трех человек, на рисунке 1 б) – сигнал после его фильтрации полосовым фильтром Баттерворта 2-го порядка с частотами среза 10 и 40 Гц.

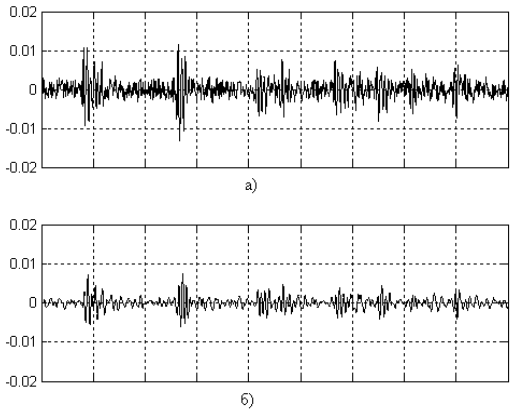


Рисунок 1. – Сейсмические сигналы группы нарушителей из трех человек до фильтрации (а) и после полосовой фильтрации (б)

Анализируя рисунок 1, можно сделать вывод, что результаты фильтрации традиционным методом нельзя признать удовлетворительными.

Удалять шумы с использованием вейвлетов возможно двумя способами. Первый из них аналогичен полосовой фильтрации. Он заключается в разложении исходного сигнала на аппроксимирующие и детализирующие коэффициенты

разных уровней по пирамидальному алгоритму Малла и последующему восстановлению сигнала по одному из коэффициентов на определенном уровне вейвлет-декомпозиции. Здесь необходимо заметить, что полосовая фильтрация в данном случае носит ограниченный характер ввиду того, что частоты среза фильтра всегда кратны частоте дискретизации сигнала и имеют фиксированные значения (fs/2, fs/4, fs/8 и т.д., где fs – частота дискретизации сигнала). Следовательно, к уже указанным выше недостаткам полосовой фильтрации добавится и этот новый недостаток, что приведет к ухудшению результатов фильтрации. Таким образом, данный способ фильтрации шумов с использованием вейвлетов не даст лучших результатов.

Гораздо более интересен второй способ вейвлет-фильтрации – ограничение уровня детализирующих коэффициентов. Кратковременные особенности сигнала, в том числе и шумы, создают детализирующие коэффициенты вейвлет-разложения с высоким содержанием компонент, имеющих большие случайные выбросы значений амплитуды. Задав некоторый порог для их уровня и срезав по уровню детализирующие коэффициенты, можно уменьшить уровень шумов. При этом возможно как глобальное ограничение всех коэффициентов по уровню, так и локальное ограничение. Более того, возможны разные типы порогов ограничения: мягкий в виде одной вертикальной ступеньки передаточной характеристики ограничения или жесткий в виде дополнительных горизонтальных полочек.

Результат фильтрации зависит от уровня вейвлет-декомпозиции сигнала, от типа порога, от метода определения порога и от типа вейвлета, используемого для удаления шума. В результате экспериментального применения вейвлет-фильтрации было установлено, что лучшим для анализа сейсмических сигналов является вейвлет Добеши 3-го порядка.

По сравнению с частотной фильтрацией, вейвлет-фильтрация имеет одно заметное преимущество – возможность ограничения уровня шума во всех частотных диапазонах, в том числе и в эффективной полосе частот полезного сигнала, что принципиально невозможно при частотной фильтрации. Благодаря этому преимуществу, теоретически, результаты фильтрации с использованием вейвлетов должны быть лучше. Для примера очистим от шума тот же самый сейсмический сигнал группы нарушителей. Результаты следующие:

1. вейвлет-фильтрация не привела к ослаблению полезного сигнала, что также является ее заметным преимуществом перед частотной фильтрацией;
2. шум в моменты времени между ударами ног нарушителей удалился практически полностью.

Однако необходимо заметить, что вейвлет-фильтрация сигналов с разложением на достаточно большое число уровней способна привести к потере информации об идентифицируемом объекте. Поэтому при удалении шумов данным способом необходимо учитывать этот фактор.

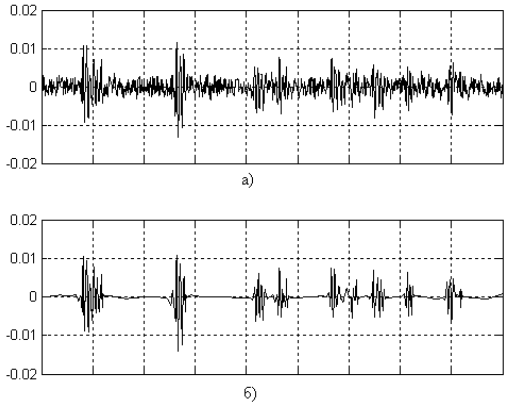


Рисунок 2. – Сейсмический сигнал группы нарушителей из трех человек до фильтрации (а) и после вейвлет-фильтрации (б)

Оценим эффективность вейвлет-фильтрации на следующем примере: возьмем смоделированный сейсмический сигнал группы нарушителей без шума, сложим его с реальным сейсмошумом, выполним вейвлет-фильтрацию полученного зашумленного сигнала и сравним исходный сигнал с результатом фильтрации.

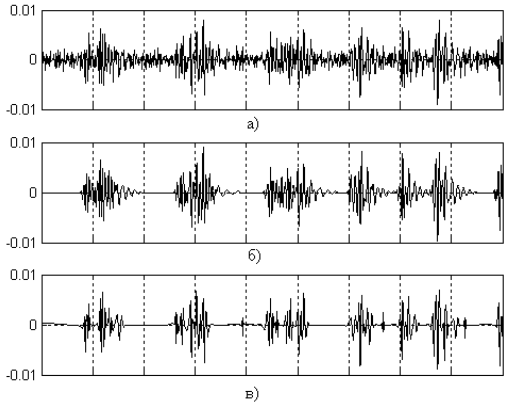


Рисунок 3. – Сейсмические сигналы группы нарушителей: зашумленные сигналы (а), незашумленные сигналы (б), сигналы после вейвлет-фильтрации (в)

Как видно из рисунка 3, шум удалился достаточно хорошо. Также можно отметить, что каждый шаг человека после фильтрации четко виден.

Таким образом, вейвлет-фильтрация является более эффективным способом удаления шумов из сейсмосигналов, чем традиционный метод – использование частотных фильтров. Однако при выборе метода удаления шума необходимо помнить, что принципиально важным фактором является то, что фильтрация не должна привести к потере полезной информации об идентифицируемом объекте.

ЛИТЕРАТУРА:

1. Отчет по НИР «Разработка графического интерфейса пользователя для имитационного моделирования сейсмосигналов», шифр «Интерфейс 2». ПГУ, Пенза, 2003.

Материалы поступили 10.12.2004. Опубликовано в Internet 20.12.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С. 71-80. Секция-3: Нормативное, методологическое и методическое обеспечение информационной безопасности.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/017)

ОЦЕНКА ЭФФЕКТИВНОСТИ МЕЖСИМВОЛЬНОГО ПЕРЕМЕЖЕНИЯ В КАНАЛАХ С РЕЛЕЕВСКИМИ ЗАМИРАНИЯМИ

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

На основе ранее разработанной динамической модели радиоканала с релеевскими замираниями [1, 2] в работе получены оценки основных показателей эффективности применения декаметрового радиоканала при использовании блочного межсимвольного перемежения. Полученные оценки позволяют определить минимальный интервал декорреляции ошибок и требуемые параметры радиоканала, необходимые для достижения наибольшей помехоустойчивости.

I. Оценка помехоустойчивости перемежения

Помехоустойчивость приема сообщений в цифровых каналах основана на оценке вероятности ошибочного приема кодовой комбинации. В общем случае в цифровых каналах применяется избыточный канальный код. Использование избыточного кодирования позволяет повысить помехоустойчивость каналов до любого значения за счет возможности обнаружения и исправления ошибок [3, 4]. Однако в силу физических особенностей декаметровых радиоканалов, моделируемых как канал с релеевскими замираниями [5] избыточное кодирование используется неэффективно. Это связано с группированием ошибок в моменты замираний, для исправления которых требуется очень большая избыточность. С другой стороны в момент усиления сигнала количество ошибок минимально, что делает нецелесообразным использование канальных кодов с большой избыточностью, так как при этом снижается канальная скорость передачи информации. Если же использовать канальный код с избыточностью соответствующей средней вероятности ошибки бита информации, как это применяется в радиоканалах действующего парка, в моменты замираний кодовые комбинации будут искажены, а в момент усиления сигналы будут приниматься без искажений. При этом в целом принятые оценки помехоустойчивости будут не адекватно отражать реальную действительность: фактическое число пораженных кодовых комбинаций будет больше расчетных, т. е. требуются более точные оценки.

Определим оценку помехоустойчивости в каналах с релеевскими замираниями, используя разработанную динамическую модель [1, 2]. В качестве элементарной вероятности помехоустойчивости каналов используется средняя вероятность ошибки приема одной элементарной посылки. Рассмотрим вариант применения каналов с двухпозиционной частотной манипуляцией, широко используемой как наиболее помехоустойчивой в декаметровом диапазоне волн, вероятность элементарной ошибки которой при известном отношении уровней мощности сигнала к помехе на входе приемника γ определяется выражением [4]

$$p_{о.чм} = \frac{e^{-\frac{\gamma}{2}}}{2\gamma}. \qquad (1)$$

Известно, что в случае релеевских замираний плотность распределения уровня принимаемого сигнала и соответственно отношения мощностей сигнала в помехе определяется выражением [4-6]

$$w(\gamma) = \frac{e^{-\frac{\gamma}{\gamma_o}}}{\gamma}. \qquad (2)$$

В результате, при релеевских замираниях средняя вероятность ошибки определяется байесовским выражением полной вероятности [7]: вероятностью ошибки при не превышении уровня сигнала выше медианного значения:

$$\overline{p}_{о\text{-}чм} = \int_0^{\gamma_m} w(\gamma) P_o(\gamma) d\gamma = \int_0^{\gamma_m} e^{-\frac{\gamma}{\gamma_o}} \frac{e^{-\frac{\gamma}{2}}}{2\gamma} d\gamma = \int_0^{\gamma_m} \frac{e^{-\frac{\gamma(2+\gamma_o)}{2\gamma_o}}}{2\gamma} d\gamma, \qquad (3)$$

где γ_o – математическое ожидание отношения уровней мощности сигнала к помехе;

γ_m – медианное значение отношения уровней мощности сигнала к помехе;

$\gamma_m = -\gamma_o \ln(0,5)$.

Вычислим интеграл (3) методом подстановки: $-\frac{\gamma(2+\gamma_o)}{2\gamma_o} = t$,

$-\frac{d\gamma(2+\gamma_o)}{2\gamma_o} = dt$:

$$\overline{p}_{о\text{-}чм} = \frac{1}{\gamma_o + 2} \int_{-\frac{\gamma_m(\gamma_o+2)}{2\gamma_o}}^{0} e^t dt = \frac{1 - e^{-\frac{\gamma_m(\gamma_o+2)}{2\gamma_o}}}{\gamma_o + 2}.$$

С учетом значения $\gamma_m = -\gamma_o \ln(0,5)$, средняя вероятность ошибки приема элемента сигнала при замирании определяется выражением

$$\overline{p}_{о\text{-}чм} = \frac{1 - 0,5^{\frac{\gamma_o+2}{2}}}{\gamma_o + 2}. \qquad (4)$$

Пользуясь аналогичными рассуждениями, определим среднюю вероятность ошибки в момент усиления сигнала, которая определяется вероятностью ошибки при превышении уровня сигнала выше медианного значения:

$$\overline{p}_{о+чм} = \int_{\gamma_m}^{¥} w(\gamma) p_o(\gamma) d\gamma = \int_{\gamma_m}^{¥} \frac{e^{-\frac{\gamma(2+\gamma_o)}{2\gamma_o}}}{2\gamma} d\gamma \,. \qquad (5)$$

Используя тот же метод с подстановкой значения $\gamma_m = -\gamma_o \ln(0,5)$, получим:

$$\overline{p}_{о+чм} = \frac{1}{\gamma_o + 2} \int_{-¥}^{-\frac{\gamma_m(\gamma_o+2)}{2\gamma_o}} e^t dt = \frac{e^{-\frac{\gamma_m(\gamma_o+2)}{2\gamma_o}}}{\gamma_o + 2} \,. \qquad (6)$$

И окончательно после подстановки значения $\gamma_m = -\gamma_o \ln(0,5)$, средняя вероятность ошибки приема элемента сигнала в момент усиления будет определяться выражением

$$\overline{p}_{о+чм} = \frac{0,5^{\frac{\gamma_o+2}{2}}}{\gamma_o + 2} \,. \qquad (7)$$

Учитывая использование каналов связи действующих радиолиний с малой избыточностью, рассмотрим вариант без избыточного кода. В случае без избыточного канального кода вероятность ошибки приема кодовой комбинации в канале с релеевскими замираниями определяется обобщенным выражением

$$P_{кк.о} = 1 - \prod_{m=1}^{n} \left(P_{З.m} \overline{q}_{о-/з} + P_{У.m} \overline{q}_{о+/у} \right), \qquad (8)$$

где $P_{З.m}$ – априорная вероятность попадания m – бита кодовой комбинации на участок замирания;

$P_{У.m}$ – априорная вероятность попадания m – бита кодовой комбинации на участок усиления;

$\overline{q}_{о-/з}$ – условная вероятность безошибочного приема одного бита информации при условии попадания m-го бита кодовой комбинации на участок замирания; $\overline{q}_{о-/з} = 1 - \overline{p}_{о-}$, где $\overline{p}_{о-}$ определяется по формуле (4), при этом для упрощения в обозначении $\overline{p}_{о-чм}$ индекс «ЧМ» опускается;

$\overline{q}_{о+/у}$ – условная вероятность безошибочного приема одного бита информации при условии попадания m-го бита кодовой комбинации на участок усиления;

$\overline{q}_{о+/у} = 1 - \overline{p}_{о+}$, где $\overline{p}_{о+}$ определяется по формуле (7), при этом для упрощения в обозначении $\overline{p}_{о+чм}$ индекс «ЧМ» также опускается;

n – длина кодовой комбинации.

Определим априорные вероятности $P_{З.m}$ и $P_{У.m}$. Для разработанной модели интервалы участков замирания и усиления следуют строго последовательно друг за другом. При этом сами интервалы распределены по экспоненциальному закону с интенсивностью смены $\lambda_з = 1/\tau_з$ (рисунок 1). Следовательно, поток переключений в то или иное состояние радиоканала будет пуассоновским [7].

Исходя из этого, число смен состояний k на определенном интервале времени T будет распределено по закону Пуассона [7]:

$$p_k = \frac{(\lambda T)^k}{k!} e^{-\lambda T}. \qquad (9)$$

Используя формулу (9), определим вероятность попадания m-го бита кодовой комбинации на интервал замирания (см. рисунок 1), с учетом, что в начальных условиях канал находился на участке замирания $p_з(0) = 1$:

$$P_{з.m} = e^{-\lambda_з \tau_0 [(m-1)d+1]} \sum_{k=1}^{\infty} \frac{\left(\lambda_з \tau_0 [(m-1)d+1]\right)^{2k}}{(2k)!}, \qquad (10)$$

где τ_0 – длительность элементарной посылки передаваемой информации;

d – интервал декорреляции, используемый при перемежении каждого бита информации.

С учетом сходимости ряда [8]: $\sum_{k=1}^{\infty} \frac{x^{2k}}{(2k)!} = \mathrm{ch}(x)$, выражение (10) можно записать:

$$P_{з.m} = \mathrm{ch}\left(\lambda_з \tau_0 [(m-1)d+1]\right) e^{-\lambda_з \tau_0 [(m-1)d+1]}. \qquad (11)$$

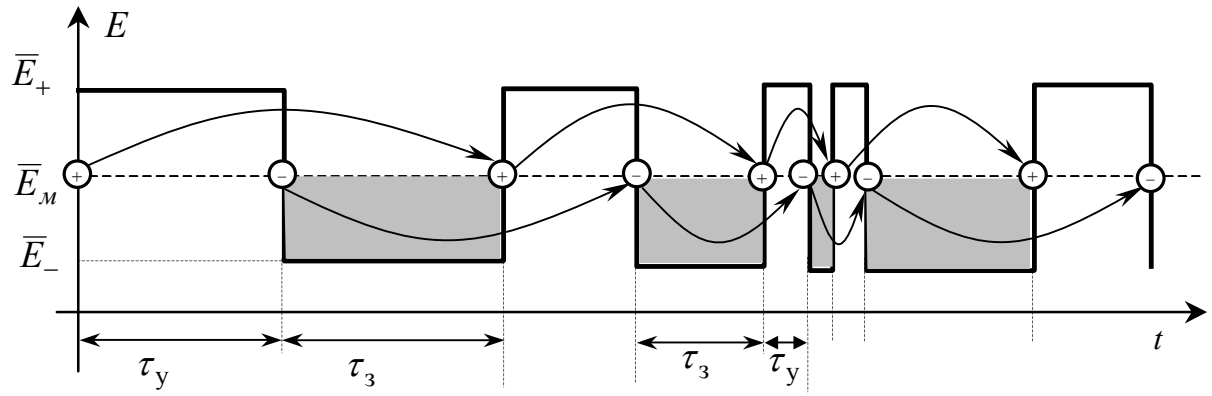


Рисунок 1. – Пояснение процесса смены состояний в канале с замираниями, где $\overline{E}_+$ – средний уровень поля в точке приема в момент усиления; $\overline{E}_-$ – уровень поля в момент замирания; $\overline{E}_м$ – медианный уровень

Аналогично, пользуясь выражением (9), определим вероятность попадания m-го бита кодовой комбинации на интервал усиления (см. рисунок 1) при $p_з(0) = 1$:

$$P_{у.m} = e^{-\lambda_з \tau_0 [(m-1)d+1]} \sum_{k=1}^{\infty} \frac{\left(\lambda_з \tau_0 [(m-1)d+1]\right)^{2k-1}}{(2k-1)!}. \qquad (12)$$

С учетом сходимости ряда [8]: $\sum_{k=1}^{\infty}\frac{x^{2k-1}}{(2k-1)!}=\mathrm{sh}(x)$, выражение (12) можно записать:

$$P_{\text{у}.m}=\mathrm{sh}\left(\lambda_{\text{з}}\tau_0[(m-1)d+1]\right)e^{-\lambda_{\text{з}}\tau_0[(m-1)d+1]} \tag{13}$$

Подставим полученные выражения априорных вероятностей состояний (11) и (13) в формулу (8). Преобразуем вначале сумму:

$$P_{\text{з}.m}\overline{q}_{\text{о-/з}}+P_{\text{у}.m}\overline{q}_{\text{о+/у}}=\overline{q}_{\text{о-/з}}\mathrm{ch}\left(\lambda_{\text{з}}\tau_0[m-1)d+1]\right)e^{-\lambda_{\text{з}}\tau_0[m-1)d+1]}+$$

$$+\overline{q}_{\text{о+/у}}\mathrm{sh}\left(\lambda_{\text{з}}\tau_0[(m-1)d+1]\right)e^{-\lambda_{\text{з}}\tau_0[m-1)d+1]}=$$

$$=\left(\frac{\overline{q}_{\text{о-/з}}(e^{\lambda_{\text{з}}\tau_0[(m-1)d+1]}+e^{-\lambda_{\text{з}}\tau_0[(m-1)d+1]})}{2}\right)e^{-\lambda_{\text{з}}\tau_0[m-1)d+1]}+$$

$$+\left(\frac{\overline{q}_{\text{о+/у}}(e^{\lambda_{\text{з}}\tau_0[(m-1)d+1]}-e^{-\lambda_{\text{з}}\tau_0[(m-1)d+1]})}{2}\right)e^{-\lambda_{\text{з}}\tau_0[m-1)d+1]}=$$

$$=\frac{\overline{q}_{\text{о-/з}}+\overline{q}_{\text{о+/у}}+(\overline{q}_{\text{о-/з}}-\overline{q}_{\text{о+/у}})e^{-2\lambda_{\text{з}}\tau_0[(m-1)d+1]}}{2}.$$

Откуда:

$$P_{\text{кк.о}}=1-\prod_{m=1}^{n}0,5\left(\overline{q}_{\text{о-/у}}+\overline{q}_{\text{о+/у}}+(\overline{q}_{\text{о-/у}}-\overline{q}_{\text{о+/у}})e^{-2\lambda_{\text{з}}\tau_0[(m-1)d+1]}\right). \tag{14}$$

Выразив $\overline{q}_{\text{о}}$ через $\overline{p}_{\text{о}}$, выражение (14) можно записать:

$$P_{\text{кк.о}}=1-\prod_{m=1}^{n}0,5\left(2-(\overline{p}_{\text{о-}}+\overline{p}_{\text{о+}})-(\overline{p}_{\text{о-}}-\overline{p}_{\text{о+}})e^{-2\lambda_{\text{з}}\tau_0[(m-1)d+1]}\right). \tag{15}$$

Следует заметить, что при $\gamma_{\text{о}}>>1$, $\overline{p}_{\text{о+}}<<\overline{p}_{\text{о-}}$, в связи с чем выражение (15) можно заменить приближенной формулой

$$P_{\text{кк.о}}\approx 1-\prod_{m=1}^{n}\left(1-0,5\overline{p}_{\text{о-}}(1+e^{-2\lambda_{\text{з}}\tau_0[(m-1)d+1]})\right). \tag{16}$$

Для упрощения анализа функции (16) перейдем к асимптотическому выражению. Сделаем следующее преобразование выражения (16):

$$\ln\left(1-P_{\text{кк.о}}\right)=\ln\left[\prod_{m=1}^{n}\left(1-0,5\overline{p}_{\text{о-}}(1+e^{-2\lambda_{\text{з}}\tau_0[(m-1)d+1]})\right)\right]=$$

$$\sum_{m=1}^{n}\ln\left[1-0,5\overline{p}_{\text{о-}}(1+e^{-2\lambda_{\text{з}}\tau_0[(m-1)d+1]})\right]\ .$$

С учетом асимптотического приближения: $\ln(1-x)\approx x$, при $x<<1$ [8], данное выражение можно записать:

$$P_{\text{кк.о}}\approx 0,5\sum_{m=1}^{n}\left(\overline{p}_{\text{о-}}(1+e^{-2\lambda_{\text{з}}\tau_0[(m-1)d+1]})\right). \tag{16}$$

Подставив в выражение (16) соответствующие значения вероятности ошибки элемента сигнала из формул (8) и (9), получим:

$$P_{\text{кк.о.чм}} \approx \frac{1-0,5^{\frac{\gamma_o+2}{2}}}{2(\gamma_o+2)} \sum_{m=1}^{n} \left(1+e^{-2\lambda_з \tau_0 [(m-1)d+1]}\right) =$$

$$= \frac{1-0,5^{\frac{\gamma_o+2}{2}}}{2(\gamma_o+2)} \left[n + \sum_{m=1}^{n} e^{-2\lambda_з \tau_0 [(m-1)d+1]} \right].$$

Откуда с учетом применения для второго слагаемого формулы суммы геометрической прогрессии [8] данное выражение примет вид (рисунок 2):

$$P_{\text{кк.о.чм}} \approx \frac{0,5-0,5^{\frac{\gamma_o}{2}+2}}{\gamma_o+2} \left[n + e^{-2\lambda_з \tau_0} \frac{1-e^{-2\lambda_з \tau_0 dn}}{1-e^{-2\lambda_з \tau_0 d}} \right]. \qquad (17)$$

Из рисунка 2 видно, что крутизна спада при перемежении достигается на более высоких скоростях манипуляции, исходя из чего следует, что использование метода перемежения будет наиболее эффективным при наименьших значениях τ_0.

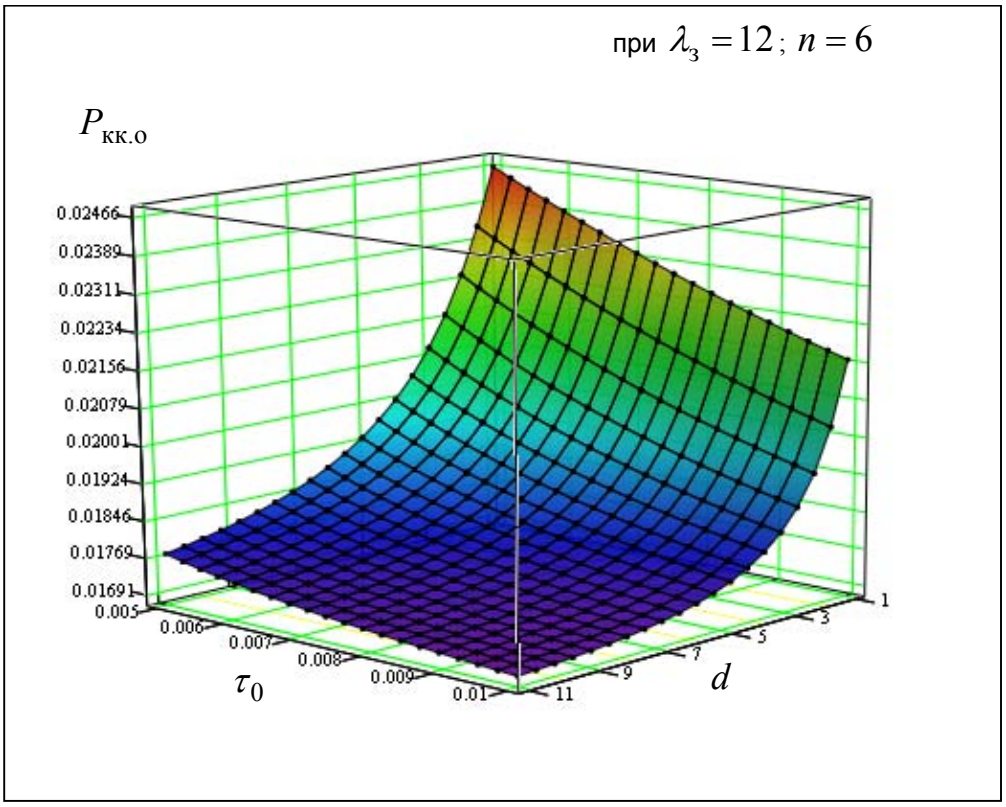


Рисунок 2. – Повышение помехоустойчивости при перемежении

II. Оценка выигрыша перемежения по помехоустойчивости

Из полученного выражения (17) определим выигрыш по помехоустойчивости:

$$\eta_{\text{о}} = \frac{P_{\text{кк.о(без перемеж)}}}{P_{\text{кк.о(с перемеж)}}} = \frac{\dfrac{0,5-0,5^{\frac{\gamma_{\text{о}}}{2}+2}}{\gamma_{\text{о}}+2}\left[n+e^{-2\lambda_{\text{з}}\tau_0}\dfrac{1-e^{-2\lambda_{\text{з}}\tau_0 n}}{1-e^{-2\lambda_{\text{з}}\tau_0}}\right]}{\dfrac{0,5-0,5^{\frac{\gamma_{\text{о}}}{2}+2}}{\gamma_{\text{о}}+2}\left[n+e^{-2\lambda_{\text{з}}\tau_0}\dfrac{1-e^{-2\lambda_{\text{з}}\tau_0 dn}}{1-e^{-2\lambda_{\text{з}}\tau_0 d}}\right]} =$$

$$= \frac{n+e^{-2\lambda_{\text{з}}\tau_0}\dfrac{1-e^{-2\lambda_{\text{з}}\tau_0 n}}{1-e^{-2\lambda_{\text{з}}\tau_0}}}{n+e^{-2\lambda_{\text{з}}\tau_0}\dfrac{1-e^{-2\lambda_{\text{з}}\tau_0 dn}}{1-e^{-2\lambda_{\text{з}}\tau_0 d}}}.$$

Данное выражение для упрощения запишем:

$$\eta_{\text{о}} \approx \frac{E_1}{E(d)}, \tag{18}$$

где $E_1 = n + e^{-2\lambda_{\text{з}}\tau_0}\dfrac{1-e^{-2\lambda_{\text{з}}\tau_0 n}}{1-e^{-2\lambda_{\text{з}}\tau_0}}$;

$E(d) = n + e^{-2\lambda_{\text{з}}\tau_0}\dfrac{1-e^{-2\lambda_{\text{з}}\tau_0 dn}}{1-e^{-2\lambda_{\text{з}}\tau_0 d}}$.

Из выражения (18) следует, что выигрыш по помехоустойчивости не зависит от энергетических характеристик канала, а определяется характеристиками среды распространения радиоволн $\lambda_{\text{з}}$, параметрами перемежения и установленной скоростью манипуляции (рисунок 3 и рисунок 4).

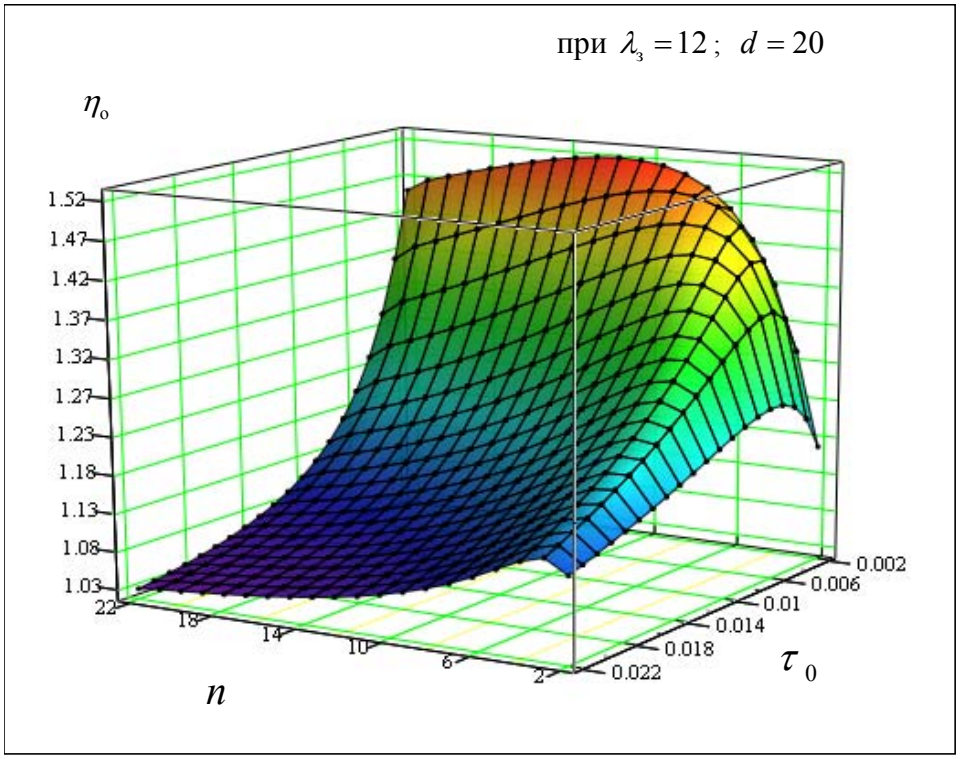


Рисунок 3. – Выигрыш по помехоустойчивости при перемежении

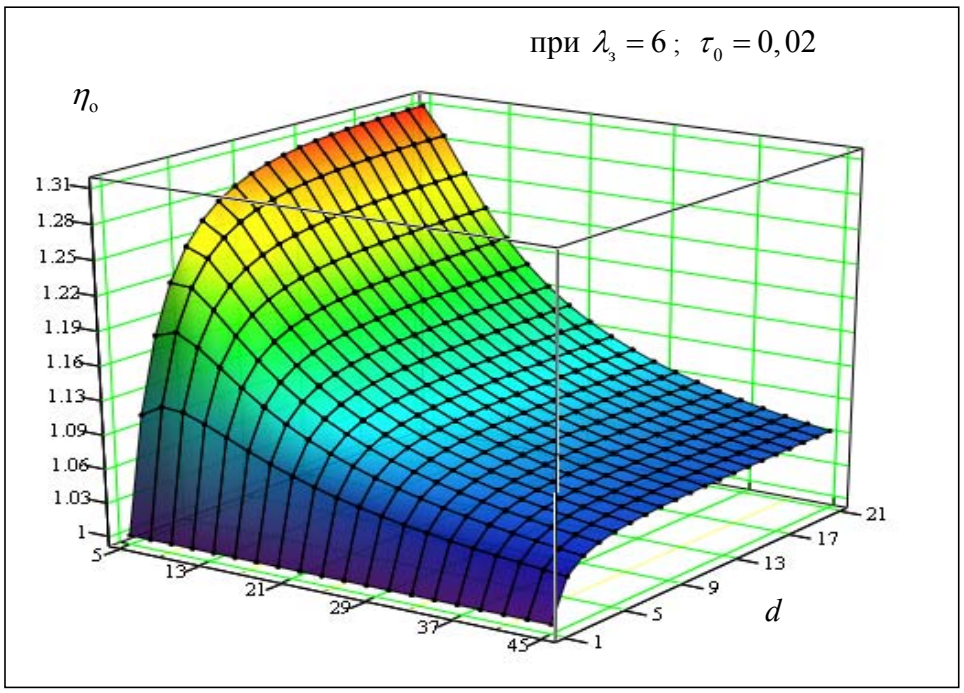


Рисунок 4. – Выигрыш по помехоустойчивости при перемежении

В данном случае при фиксированных параметрах среды распространения радиоволн существуют оптимальные параметры радиоканала (скорость манипуляции и длина канального кода): большей скорости манипуляции соответствует более длинный канальный код (см. рисунок 3). Кроме того, следует заметить, что кодам меньшей длины соответствует больший минимальный интервал декорреляции (см. рисунок 4).

III. Оценка энергетического выигрыша за счет перемежения

Определим энергетический выигрыш при перемежении, для чего выражение (17) выразим через $\gamma_о$:

$$\gamma_о = \frac{0,5 - 0,5^{\frac{\gamma_о}{2}+2}}{P_{кк.о.чм}} \left[n + e^{-2\lambda_з \tau_0} \frac{1 - e^{-2\lambda_з \tau_0 dn}}{1 - e^{-2\lambda_з \tau_0 d}} \right] - 2 .$$

Учитывая применение каналов при больших отношениях мощностей сигнала к шуму $\gamma_о >> 1$, величина $0,5 >> 0,5^{\frac{\gamma_о}{2}+2}$, в связи с чем полученное выражение примет вид

$$\gamma_о = \frac{E(d)}{2P_{кк.о.чм}} - 2 . \qquad (19)$$

Определим энергетический выигрыш при перемежении:

$$\eta_Р = \frac{\gamma_{о(без\ перемеж)}}{\gamma_о(d)} = \frac{(E_1 / 2P_{кк.о.чм}) - 2}{(E(d) / 2P_{кк.о.чм}) - 2} . \qquad (20)$$

Из данного выражения следует, что энергетический выигрыш зависит от требуемой помехоустойчивости и, прежде всего, от установленной скорости

манипуляции и длины кода при заданных характеристиках среды распространения радиоволн (рисунок 5).

Из рисунка 5 видно, что при заданных характеристиках среды распространения радиоволн существует определенный максимум соответствующий определенной скорости манипуляции и длине канального кода. Кроме того, этот максимум энергетического выигрыша возрастает с увеличением скорости манипуляции, которому соответствует более большее значение длины канального кода (см. рисунок 5). Исследование влияния требуемой помехоустойчивости кодовой комбинации $P_{\text{кк.о}}$ показал слабое влияние этого параметра на энергетический выигрыш $\eta_{\text{Р}}$.

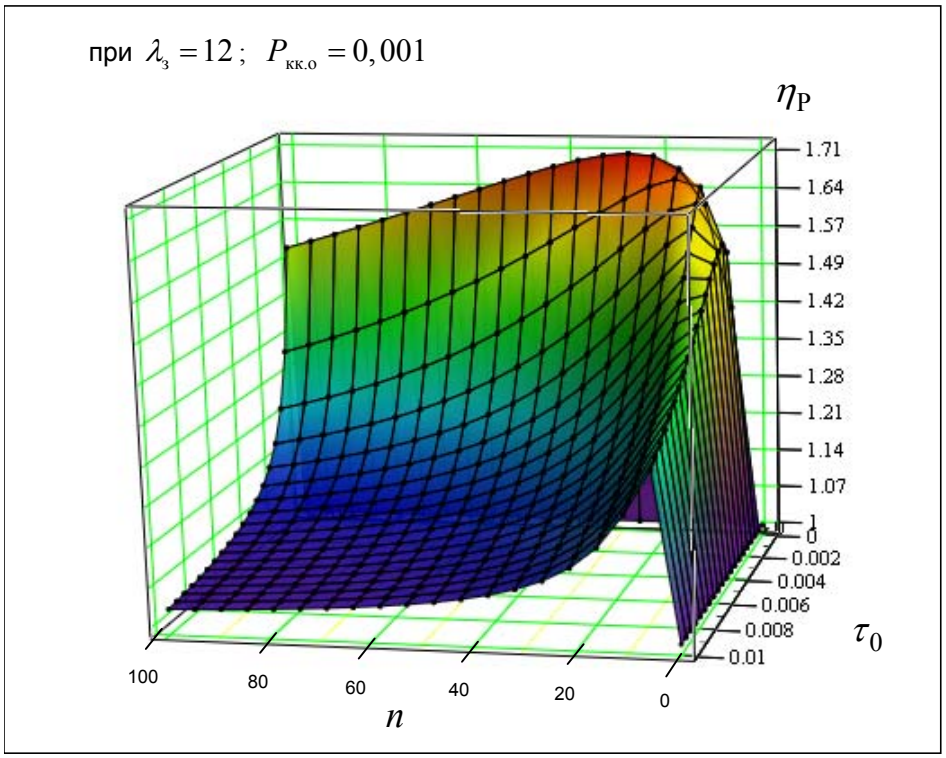


Рисунок 5. – Энергетический выигрыш при перемежении

Выводы:

1. Наибольшая эффективность межсимвольного перемежения достигается при большей скорости манипуляции и меньшей длине канального кода. При этом требуется решать компромисс, так как для достижения максимального выигрыша большей скорости манипуляции соответствует большая длина канального кода.
2. Канальным кодам меньшей длины соответствует больший интервал декорреляции, т.е. с увеличением длины кода эффективность использования метода межсимвольного перемежения в декаметровых радиоканалах снижается.

ЛИТЕРАТУРА:

1. Орощук И.М. Динамическая модель релеевского канала с замираниями // Журнал радиоэлектроники. – 2002. – № 10. – 10 с. http://www.jre.cplire.ru/jre/oct02/index.html
2. Орощук И.М., Воронов М.В. Метод статистического обнаружения воздействий имитопомех // НТК «Безопасность информационных технологий»: Труды НТК. Том 4. Секция 3: «Нормативное, методологическое

и методическое обеспечение информационной безопасности». 8 июня 2003 – г. Пенза, ПНИЭИ. – 2003. – С. 14–24.
3. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра: Пер. с англ. / Под ред. В.И. Журавлева. – М.: Радио и связь, 2000. – 520 с
4. Финк Л.М. Теория передачи дискретных сообщений. – М.: Советское радио. 1970. – 727 с.
5. Зюко А.Г. Помехоустойчивость и эффективность систем связи. – М.: Связь, 1972. – 260 с.
6. Долуханов М.П. Флуктуационные процессы при распространении радиоволн. – М.: Связь, 1971. – 180 с.
7. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. – М.: Наука, 1991. – 384 с.
8. Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся втузов. – М.: Наука, 1986. – 544 с.

Материалы поступили 10.12.2004. Опубликовано в Internet 20.12.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С. 81-84. Секция-8: Конфиденциальность, целостность, доступность.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/018)

КОРРЕЛЯЦИОННЫЙ МЕТОД НАСТРОЙКИ КОРРЕКТОРА КАНАЛА ПРИ ВОЗДЕЙСТВИИ НЕПРЕДНАМЕРЕННЫХ АТАК

Иванов А.П. e-mail: ivanov@beda.stup.ac.ru
Султанов Б.В. e-mail: sultanov@beda.stup.ac.ru
Пензенский государственный университет

Отсутствие в сети связи общего пользования (ССОП) необходимых средств защиты в условиях информационного противоборства делает ССОП России в целом уязвимой от враждебных акций, недобросовестной конкуренции операторов связи, также криминальных и иных противоправных действий [1].

В связи с этим появились принципиально новая задача, связанная с необходимостью обеспечения заданного (гарантированного сетью) качества процесса передачи данных пользователя (например, достоверности передаваемых через сеть данных пользователя) в условиях возможных непреднамеренных и преднамеренных атак на информационную сферу ССОП.

Одним из вариантов решения данной задачи является включение в состав модемов, используемых в ССОП, корректора частотных характеристик канала.

Целью данной статьи является разработка корреляционного метода настройки корректора канала по испытательному сигналу в условиях непреднамеренных аддитивных атак на информационную сферу ССОП.

Предположим, что имеется некоторый испытательный сигнал $\{x_{\text{т}}[i]\}$ (i – номер отсчёта), представляющий собой периодическую последовательность с периодом в $N_{\text{п}}$ отсчётов, круговая (периодическая) автокорреляционная функция которой

$$B_{xx}[m]=\frac{1}{N_{\text{п}}}\sum_{l=0}^{N_{\text{п}}-1}x_{\text{т}}[l]\,x_{\text{т}}[(l+m)\bmod N_{\text{п}}] \qquad (1)$$

определяется соотношением:

$$B_{xx}[m]=\begin{cases}1 & \text{при } (m \bmod N_{\text{п}})=0\\ 0 & \text{при других } m\end{cases}. \qquad (2)$$

При прохождении этого испытательного сигнала через канал с импульсной реакцией $h(t)$ и аддитивным шумом $n_{\text{к}}$, некоррелированным с $x_{\text{т}}[i]$, отклик канала $y_{\text{к}}[i]$ можно описать выражением:

$$y_{\text{к}}[i]=\sum_{k=0}^{N_{\text{п}}-1}h[k]\,x_{\text{т}}[(i-k)\bmod N_{\text{п}}]+n_{\text{к}}[i]. \qquad (3)$$

В дальнейшем будем полагать, что шум $n_{\text{к}}[i]$ является центрированным гауссовским с дисперсией σ^2 и функцией автокорреляции вида

$$R_{\text{к}}[i]=\sigma^2\,x_0[i], \qquad (4)$$

где $x_0[i]$ – последовательность “единичный отсчёт”.

Вычислим периодическую функцию взаимной корреляции $B_{xx}[m]$ сигналов $x_{\text{т}}[i]$ и $y_{\text{к}}[i]$. По аналогии с (1) можно записать

$$B_{xy}[m]=\frac{1}{N_{\text{п}}}\sum_{l=0}^{N_{\text{п}}-1}y_{\text{к}}[l]\,x_{\text{т}}[(l+m)\bmod N_{\text{п}}]. \qquad (5)$$

Подставляя в выражение (5) значение $y_{\text{к}}[i]$, определяемое формулой (3), получаем:

$$B_{xy}[m]=\sum_{k=0}^{N_{\text{п}}-1}h[k]\frac{1}{N_{\text{п}}}\sum_{i=0}^{N_{\text{п}}-1}x_{\text{Т}}[(i-k)\bmod N_{\text{п}}]\,x_{\text{Т}}[(i+m)\bmod N_{\text{п}}]+$$
$$+\frac{1}{N_{\text{п}}}\sum_{i=0}^{N_{\text{п}}-1}n_{\text{к}}[i]\,x_{\text{Т}}[(i+m)\bmod N_{\text{п}}]. \qquad (6)$$

Обозначим первое и второе слагаемые выражения (6) соответственно как $B_{1\text{xy}}[m]$ и $B_{2\text{xy}}[m]$. Рассмотрим $B_{1\text{xy}}[m]$. С целью его упрощения осуществим во внутренней сумме замену переменной. Положим

$$l=(i-k)\bmod N_{\text{п}}, \qquad (7)$$

тогда

$$i \bmod N_{\text{п}}=(l+k)\bmod N_{\text{п}}. \qquad (8)$$

С учётом (8) получаем:

$$(i+m)\bmod N_{\text{п}}=(l+k+m)\bmod N_{\text{п}}, \qquad (9)$$

причём при изменении i от 0 до $N_{\text{п}}$-1 переменная l также пробегает все значения периода. Поэтому на основании (6), принимая во внимание (7) и (9) можно записать

$$B_{1xy}[m]=\sum_{k=0}^{N_{\text{п}}-1}h[k]\cdot\frac{1}{N_{\text{п}}}\sum_{l=0}^{N_{\text{п}}-1}x_{\text{Т}}[l]\,x_{\text{Т}}[(l+k+m)\bmod N_{\text{п}}]. \qquad (10)$$

В соответствии с (1) и (2) имеем:

$$\frac{1}{N_{\text{п}}}\sum_{l=0}^{N_{\text{п}}-1}x_{\text{Т}}[l]\,x_{\text{Т}}[(l+k+m)\bmod N_{\text{п}}]=\begin{cases}1 & \text{при } [(k+m)\bmod N_{\text{п}}]=0\\ 0 & \text{в других случаях}\end{cases}. \qquad (11)$$

При значениях m и k, удовлетворяющих неравенствам $1\le m\le N_{\text{п}}$ и $1\le k\le N_{\text{п}}$-1 (что соответствует одному периоду последовательностей $x_{\text{Т}}[i]$ и $y_{\text{к}}[i]$), из соотношения $(k+m)$ mod $N_{\text{п}}=0$ следует, что $k=N_{\text{п}}-m$.

Это означает, что для каждого m во внешней сумме выражения (10) присутствует только одно ненулевое слагаемое. Оно соответствует значениям $k=N_{\text{п}}-m$, при которых сумма (11) отлична от нуля и равна единице. В результате соотношение (10) принимает вид

$$B_{1xy}[m]=h[N_{\text{п}}-m],\ 1\le m\le N_{\text{п}}. \qquad (12)$$

Второе слагаемое соотношения (6), обусловленное наличием аддитивного шума канала $n_{\text{к}}[i]$, представляет собой случайную последовательность, определяемую выражением

$$B_{2xy}[m]=\frac{1}{N_{\text{п}}}\sum_{i=0}^{N_{\text{п}}-1}n_{\text{к}}[i]\,x_{\text{Т}}[(i+m)\bmod N_{\text{п}}]. \qquad (13)$$

Сопоставляя (13) и (1) нетрудно заметить, что $B_{2\text{xy}}[m]$ представляет собой оценку периодической функции взаимной корреляции шума $n_{\text{к}}$ и детерминированного теста $x_{\text{Т}}$. Поскольку эти величины некоррелированы, можно положить, что

$$B_{2xy}[m]\approx 0. \qquad (14)$$

Для более полного описания статистических свойств сигнала $B_{2\text{xy}}[m]$, определяющих точность выполнения приближённого равенства (14), проведём следующие рассуждения.

Прежде всего отметим, что, поскольку выражение (13) описывает линейное преобразование дискретного гауссовского процесса $n_{\text{к}}[i]$, распределение вероятностей последовательности $B_{2\text{xy}}[m]$ также будет гауссовским. Так как $\overline{n_{\text{к}}[i]}=0$, то

$$\overline{B_{2xy}[m]} = \overline{\frac{1}{N_\text{п}} \sum_{i=0}^{N_\text{п}-1} n_\text{к}[i]\, x_\text{Т}[(i+m) \bmod N_\text{п}]} = \frac{1}{N_\text{п}} \sum_{i=0}^{N_\text{п}-1} \overline{n_\text{к}[i]}\, x_\text{Т}[(i+m) \bmod N_\text{п}] = 0 .$$

Дисперсия сигнала $B_{2\text{ху}}[m]$ определяется как

$$\overline{B_{2xy}^2[m]} = \frac{1}{N_\text{п}^2} \sum_{i=0}^{N_\text{п}-1} \sum_{q=0}^{N_\text{п}-1} x_\text{Т}[(i+m) \bmod N_\text{п}]\, x_\text{Т}[(q+m) \bmod N_\text{п}] \cdot \overline{n_\text{к}[i]\, n_\text{к}[q]} . \qquad (15)$$

Для вычисления среднего $\overline{n_\text{к}[i]\, n_\text{к}[q]}$ осуществим подстановку $i=q+v$. При этом $v=i-q$, и на основании (4) имеем:

$$\overline{n_\text{к}[i]\, n_\text{к}[q]} = \overline{n_\text{к}[q+v]\, n_\text{к}[q]} = R_\text{к}[v] = \sigma^2\, x_0[v] = \sigma^2\, x_0[i-q] . \qquad (16)$$

Подставляя результат (16) в (15) и учитывая свойства последовательности, получаем:

$$\overline{B_{2xy}^2[m]} = \frac{\sigma^2}{N_\text{п}^2} \sum_{i=0}^{N_\text{п}-1} x_\text{Т}^2[(i+m) \bmod N_\text{п}] = \frac{\sigma^2}{N_\text{п}^2} \sum_{i=0}^{N_\text{п}-1} x_\text{Т}^2[i]. \qquad (17)$$

Полагая в (1) и (2) $m=0$ и переходя к новым обозначениям (приняв $l=i$), можно записать

$$1/N_\text{п} \sum_{i=0}^{N_\text{п}-1} x_\text{Т}^2[i] = 1 . \qquad (18)$$

С учётом (18) на основании (17) имеем:

$$\overline{B_{2xy}^2[m]} = \frac{\sigma^2}{N_\text{п}} \ . \qquad (19)$$

Принимая во внимание (6) и (12), объединим полученные результаты в виде выражения

$$B_{xy}[m] = h[N_\text{п} - m] + n'_\text{к}[m], \qquad (20)$$

где $n'_\text{к}[m] = B_{2xy}[m]$ – отсчёты центрированного дискретного белого гауссовского шума с дисперсией, определяемой равенством (19).

Таким образом, в установившемся режиме каждый период функции взаимной корреляции испытательного сигнала с откликом канала в соответствии с выражением (20) содержит отсчёты импульсной реакции канала. Очевидно, что период испытательного сигнала $N_\text{п}$ должен превышать максимальную ожидаемую длительность оцениваемой импульсной реакции и может быть весьма значительным. При этом с одной стороны в соответствии с (19) уменьшается мешающее влияние фигурирующего в (20) шума оценки импульсной реакции, а с другой – резко возрастает вычислительная сложность операции определения функции взаимной корреляции (5). Последнее обстоятельство делает целесообразным выполнение данной процедуры в частотной области с использованием для перехода от временных последовательностей к их спектрам и обратно алгоритмов БПФ. Общая последовательность вычислений в таком случае задаётся алгоритмом

$$\{B_{xy}[k]\} = \text{F}^{-1}\{\text{F}(\text{y}_\text{к}[\text{k}]) \cdot \text{F}^*(\text{x}_\text{Т}[\text{k}])\}, \qquad (21)$$

где F и F^{-1} – операторы прямого и обратного преобразований Фурье; *– знак комплексного сопряжения.

Отметим, что все полученные результаты (в частности, выражения (20) и (21)) справедливы лишь при наличии действительного испытательного сигнала с идеальной периодической функцией автокорреляции вида (2).

Метод настройки корректора канала заключается в следующем. В режиме вхождения в связь передается несколько периодов синтезированного испытательного сигнала [2]. Соответствующий им отклик канала $y_\text{к}[k]$ запоминается (за исключением первого периода, отражающего переходные

процессы). При этом длина периода испытательного сигнала $N_{\text{п}}$ определяется предполагаемой длительностью импульсной реакции, частотой дискретизации и уровнем шума в канале. Далее в соответствии с вытекающим из (20) и (21) алгоритмом, имеющим вид

$$\mathrm{F}\left(y_{\text{к}}[m]\right)\mathrm{F}^{*}\left(x_{\text{т}}[m]\right)=H\left(k\right)+N'_{\text{к}}\left(k\right),$$

для каждого периода отклика вычисляются отсчёты реализаций комплексной частотной характеристики (КЧХ) канала $H(k)=\mathrm{F}(h[m])$ с наложенным ДПФ фигурирующего в (20) шума корреляции $N_{\text{к}}'(k)=\mathrm{F}(n_{\text{к}}'[m])$. Затем по полученным значениям КЧХ оцениваются АЧХ и ФЧХ канала связи.

Мешающее влияние непреднамеренной аддитивной атаки $N_{\text{к}}'(k)$ можно уменьшить, усредняя результаты обработки нескольких периодов отклика. Однако наличие ухода частоты несущего колебания в канале не позволяет осуществить непосредственное усреднение полученных описанным способом оценок ФЧХ. Данную проблему можно решить, вычисляя на основе этих данных характеристики группового времени прохождения (ГВП), определяемые как первая конечная разность по частоте от ФЧХ и поэтому не зависящие от фиксированного частотного сдвига.

Усреднённые значения АЧХ и ГВП сравниваются с эталонными. По результатам сравнения рассчитываются аналогичные частотные характеристики корректора канала, по которым восстанавливается его КЧХ, а затем посредством ОДПФ определяются отсчёты импульсной реакции, используемые в качестве коэффициентов исполнительного элемента – цифрового нерекурсивного фильтра.

При вычислении ДПФ и ОДПФ предполагается использование алгоритмов БПФ.

Возможности современных процессоров цифровой обработки сигналов делают вполне приемлемым объём реализационных затрат, предполагаемых при применении предложенного метода. Практическая его апробация позволила осуществить коррекцию частотных характеристик канала с точностью до одного ППУ в диапазоне от 1 до 15 ППУ за время порядка 1,5 с. в модеме [3], в настоящее время серийно выпускаемом отечественной промышленностью.

ЛИТЕРАТУРА:

1. Концепция информационной безопасности Сетей связи общего пользования Взаимоувязанной сети связи Российской Федерации [Электронный ресурс]: Проект. – Москва, 2002. – Режим доступа: http://daily.sec.ru
2. Иванов А.П., Султанов Б.В. Синтез испытательного сигнала для настройки корректора канала//Безопасность информационных технологий. Труды научно-технической конференции. Том 5. – Пенза: ПГУ, 2005.
3. Бочков В.К., Кирюхин М.С., Лысиков А.В. и др. Двухпроводный дуплексный модем // Электросвязь. – 2000. – №7. – с. 35–38.

Материалы поступили 12.12.2004. Опубликовано в Internet 20.12.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С. 85-88. Секция-5: Управление информационной безопасностью.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/019)

СИНТЕЗ ИСПЫТАТЕЛЬНОГО СИГНАЛА ДЛЯ НАСТРОЙКИ КОРРЕКТОРА КАНАЛА

Иванов А.П. e-mail: ivanov@beda.stup.ac.ru
Султанов Б.В. e-mail: sultanov@beda.stup.ac.ru
Пензенский государственный университет

Одним из важнейших параметров систем передачи данных по коммутируемым каналам связи с высокой удельной скоростью является время вхождения в связь, определяемое, в том числе временем настройки корректора канала. Для быстрой подготовки канала связи к передаче данных настройка корректора должна производится за время, соизмеримое со временем установления автоматического соединения, т.е. за время порядка 1-2 секунд. За указанное время корректор канала может быть настроен только по испытательному сигналу.

Целью данной статьи является синтез испытательного сигнала для настройки корректора канала входящего в состав приемной части модема.

Предположим, что имеется некоторый испытательный сигнал $\{x_{\text{Т}}[i]\}$ (i – номер отсчёта), представляющий собой периодическую последовательность с периодом в $N_{\text{п}}$ отсчётов, круговая (периодическая) автокорреляционная функция которой

$$B_{xx}[m]=\frac{1}{N_{\text{п}}}\sum_{l=0}^{N_{\text{п}}-1}x_{\text{Т}}[l]\,x_{\text{Т}}[(l+m)\bmod N_{\text{п}}] \qquad (1)$$

определяется соотношением:

$$B_{xx}[m]=\begin{cases}1 & \text{при } (m \bmod N_{\text{п}})=0\\ 0 & \text{при других } m\end{cases}. \qquad (2)$$

В работе [1] показана невозможность построения апериодической последовательности конечной длины $\{x_{\text{а}}[i]\}$, содержащей $N_{\text{а}}$ отсчётов, с идеальной функцией автокорреляции

$$B_{\text{а}xx}[m]=1/(N_{\text{а}}-m)\sum_{l=0}^{N_{\text{а}}-m-1}x_{\text{а}}[l]\,x_{\text{а}}[l+m] \qquad (3)$$

вида

$$B_{\text{а}xx}[m]=\begin{cases}1 & \text{при } m=0\\ 0 & \text{при } m\neq 0\end{cases}. \qquad (4)$$

Действительно, поскольку хотя бы первый $x_{\text{а}}[0]$ и последний $x_{\text{а}}[N_{\text{а}}\text{-}1]$ отсчёты сигнала $\{x_{\text{а}}[i]\}$ отличны от нуля, то кроме первого (соответствующего m=0) по крайней мере ($N_{\text{а}}$-1)-й отсчёт функции $B_{\text{а}xx}[m]$ также является ненулевым, так как в соответствии с (3)

$$B_{\text{а}xx}[N_{\text{а}}-1]=x_{\text{а}}[N_{\text{а}}-1]\,x_{\text{а}}[0]\neq 0\,.$$

Это означает принципиальную невыполнимость условия (4) идеальности автокорреляционной функции. Однако приведённые рассуждения отнюдь не исключают возможность реализации периодического испытательного сигнала $\{x_{\text{Т}}[i]\}$ с определяемой выражением (1) идеальной круговой автокорреляционной функцией вида (2), поскольку независимо от значения m в сумме (1) всегда

присутствует одинаковое число $N_{\text{п}}$ в общем случае имеющих разные знаки слагаемых.

Различные варианты построения комплексных периодических дискретных сигналов с $B_{xx}[m]$ вида (2) были предложены в ряде работ зарубежных авторов. Однако необходимый для измерения частотных характеристик канала связи сигнал $\{x_{\text{Т}}[i]\}$ должен быть действительным, так как импульсная реакция исследуемого тракта вещественна. Использование для этой цели известных псевдослучайных сигналов (или M-последовательностей), приводит к неоправданным дополнительным погрешностям эксперимента, поскольку для них соотношение (2) выполняется лишь приблизительно.

В связи с этим рассмотрим задачу синтеза действительного периодического испытательного сигнала с идеальной круговой автокорреляционной функцией вида (2).

В соответствии с теоремой Винера-Хинчина дискретный энергетический спектр $G_x[k]$ (k – номер отсчёта спектра) искомого сигнала можно определить, вычисляя ДПФ от обеих частей равенства (2). При этом получаем:

$$G_x[k] = \sum_{m=0}^{N_{\text{п}}-1} B_{xx}[m] \exp\{- j\,(2\pi / N_{\text{П}})\, k\, m\} = 1\,.$$

Таким образом, $G_x[k]$ является равномерным и единичным. Это означает, что спектр амплитуд последовательности $\{x_{\text{Т}}[i]\}$ также является равномерным и единичным. Вид спектра фаз не оказывает влияния на автокорреляционную функцию, но во многом определяет форму синтезированного испытательного сигнала, которую удобно характеризовать с помощью пик-фактора. Исследования показали, что минимальный пик-фактор может быть получен при изменении аргумента $\varphi_{\text{Т}}[k]$ отсчётов ДПФ испытательного сигнала по квадратичному закону

$$\varphi_{\text{Т}}[k] = \frac{2\,\pi}{N_{\text{п}}}\, k^2\,.$$

Кроме того, поскольку искомый сигнал должен быть действительным, необходимо, чтобы отсчёты его дискретного спектра удовлетворяли условиям симметрии. Исходя из изложенного, можно записать следующие соотношения, определяющие ДПФ $X_{\text{Т}}[k]$ синтезируемого сигнала:

при $N_{\text{п}}$ чётном –

$$X_{\text{Т}}[k] = \begin{cases} \exp\left(j\,(2\pi / N_{\text{П}})\, k^2 \right) & \text{при} \quad 0 \le k \le 0{,}5\, N_{\text{п}} \\ X_{\text{Т}}^{*}[N_{\text{п}} - k] & \text{при} \quad 0{,}5\, N_{\text{п}} \le k \le N_{\text{п}} - 1 \end{cases} \tag{5}$$

при $N_{\text{п}}$ нечётном –

$$X_{\text{Т}}[k] = \begin{cases} \exp\left(j\,(2\pi / N_{\text{П}})\, k^2 \right) & \text{при} \quad 0 \le k \le 0{,}5\,(N_{\text{п}} - 1) \\ X_{\text{Т}}^{*}[N_{\text{п}} - k] & \text{при} \quad 0{,}5\,(N_{\text{п}} - 1) \le k \le N_{\text{п}} - 1 \end{cases}. \tag{6}$$

Чтобы получить выражения для отсчётов сигнала $\{x_{\text{Т}}[i]\}$, необходимо вычислить ОДПФ от функций, задаваемых соотношениями (5) и (6). После выполнения всех необходимых преобразований получаем:

$$x_{\text{Т}}[i] = 1 + \left[(N_{\text{п}} + 1) \bmod 2\right] \cdot (-1)^{i + \left(\frac{N_{\text{п}}}{2} \bmod 2 \right)} + 2 \sum_{k=1}^{\left(\frac{N_{\text{п}}-1}{2} \right)_{\text{ц.ч.}}} \cos\left[(2\pi / N_{\text{П}})\, k\, (k + i) \right] \tag{7}$$

где обозначение $(\cdot)_{\text{ц.ч.}}$ соответствует целой части числа, заключённого в скобки.

В том случае, когда период $N_{\text{п}}$ необходимого испытательного сигнала является достаточно большим ($>10^4$), вычисления по формуле (7) оказываются весьма трудоёмкими и требуют значительных затрат машинного времени. Если в такой ситуации имеется возможность выбора значения $N_{\text{п}}$ равным целой степени числа 2, то более предпочтительным может оказаться другой подход к расчёту

$\{x_T[i]\}$, в соответствии с которым вначале на основе соотношения (5) следует определить отсчёты $X_T[k]$ ДПФ искомого сигнала, а затем с помощью БПФ найти ОДПФ. Поскольку в современных программных математических пакетах вычисление ДПФ и ОДПФ выполняется посредством одной команды, при их использовании данный способ расчёта $\{x_T[i]\}$ реализуется проще и экономичнее.

На рис. 1 представлен график синтезированного сигнала с периодом $N_п$=64, на котором по оси абсцисс отложены номера i, а по оси ординат – значения её отсчётов $x_T[i]$.

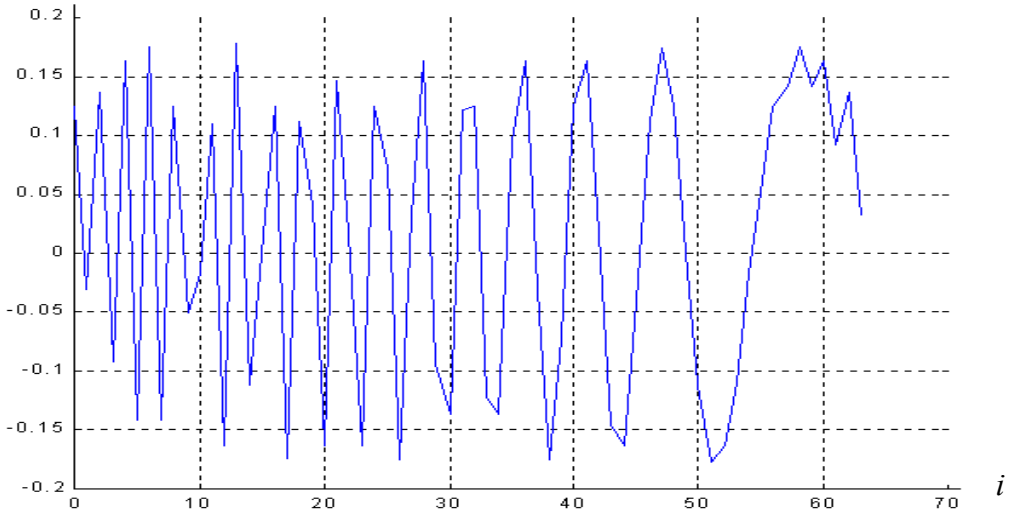


Рис. 1

Для обеспечения цельности восприятия характера изменения данного сигнала во времени отдельные точки, соответствующие отсчётам, соединены отрезками прямой линии. Вид графика показывает, что пик-фактор рассматриваемого испытательного сигнала должен быть близок к аналогичному параметру гармонического сигнала, который, как известно, равен $\sqrt{2} \approx 1.141$.

Более полная информация о значениях пик-фактора $K_{п\text{-}ф}$ и их связи с периодом сигнала $N_п$ представлена на рис. 2, на котором приведены зависимости $K_{п\text{-}ф}=f_{п\text{-}ф}(\log_2 N_{пф})$, где $N_{пн}=2^{kk}$ – число, близкое к $N_п$ и равное целой степени kk двойки.

Сплошная линия на этом рисунке соответствует случаю $N_п=N_{пн}=2^{kk}$ (то есть, $N_п$ кратно целой степени числа 2 и, следовательно, кратно 4); нижняя прерывистая линия (комбинация точек и тире) отражает ситуацию, когда $N_п=N_{пн}+2$ ($N_п$ чётно, но не кратно 4); верхняя прерывистая линия соответствует нечётным значениям $N_п = N_{пн}+1$. Из графиков видно, что у испытательных сигналов с чётным периодом пик-фактор приблизительно одинаков и удовлетворяет неравенству $K_{п\text{-}ф}<1{,}46$. У испытательных сигналов с нечётным периодом этот параметр несколько больше, но тоже принимает вполне приемлемые значения $K_{п\text{-}ф}<1{,}74$.

Расчёты, выполненные на ЭВМ, подтвердили, что во всех случаях периодическая автокорреляционная функция испытательных сигналов, определяемых формулой (7), является идеальной, задаваемой соотношением (2).

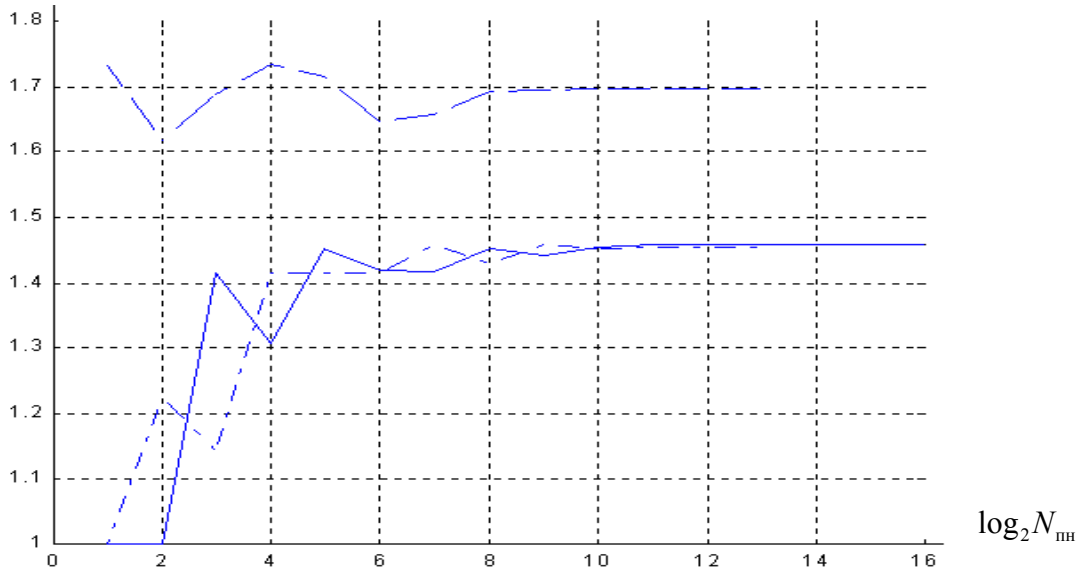


Рис. 2

ЛИТЕРАТУРА:

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

Материалы поступили 12.12.2004. Опубликовано в Internet 20.12.2004.

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.89-93. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/020)

ПРИМЕНЕНИЕ МЕТОДОВ РЕКУРРЕНТНОГО ОЦЕНИВАНИЯ ДЛЯ ИДЕНТИФИКАЦИИ БИОМЕТРИЧЕСКИХ ОБЪЕКТОВ

д.т.н. Геращенко С.И., к.т.н. Геращенко С.М., к.т.н. Лупанов М.Ю., Янкина Н.Н.

Пензенский государственный университет

Свойства биометрических объектов, способны в значительной мере изменятся, в связи с чем в системах при распознавании образов биометрических объектов процесс получения информации, обработки данных и выдачи результатов ведется в реальном масштабе времени. При этом обработка данных на каждом шаге должна завершаться до начала следующего шага. В противном случае, построенная модель исследуемого объекта не сможет справиться с потоком информации.

В этой связи весьма перспективным является применение методов рекуррентного оценивания [1], основанных на последовательной обработке измеряемых входно-выходных данных. Они позволяют отслеживать изменения, происходящие в исследуемом объекте, непосредственно в процессе измерений при априорном использовании информации, содержащейся в наблюдаемых данных.

Рекуррентные методы имеют следующие преимущества [2]:

– достаточно простая реализация;

– скромные требования к использованию оперативной памяти ЭВМ;

– эффективное использование избыточности множества экспериментальных данных для получения высокой скорости сходимости алгоритма.

Типичный рекуррентный алгоритм идентификации имеет вид:

$$\hat{\theta}(t) = \hat{\theta}(t-1) + L(t)\left(y(t) - \hat{y}(t)\right), \qquad (1)$$

где $\hat{\theta}(t)$ – оценка параметров во время t, $y(t)$ – наблюдаемый выходной сигнал во время t, $\hat{y}(t)$ – предсказатель значения $y(t)$, основанный на наблюдениях до момента времени $t-1$ и на текущей модели в момент времени $t-1$, $L(t)$ – коэффициент усиления, определяющий в каком направлении текущая ошибка предсказания $y(t)-\hat{y}(t)$ воздействует на изменение оценки параметров в соответствии с новыми данными.

Коэффициент усиления обычно определяется как

$$L(t) = Q(t)\psi(t), \qquad (2)$$

где $\psi(t)$ – градиент предсказателя $\hat{y}(t|\theta)$ по θ, $Q(t)$ – матрица, влияющая на коэффициент усиления адаптации и на направление в которым производятся изменения в соответствии с новыми данными.

Модели соответствующие линейным регрессиям, в этом случае, могут быть представлены в виде:

$$y(t) = \psi^T(t)\theta_0(t) + e(t), \tag{3}$$

где $\psi(t)$ – вектор регрессии содержащий старые значения наблюдаемых входных и выходных данных, $\theta_0(t)$ – представляет истинное описание системы, $e(t)$ – шум. Для этих моделей предсказатель имеет следующий вид:

$$\hat{y}(t) = \psi^T(t)\theta(t-1), \tag{4}$$

где $\psi(t)$ – градиент предсказателя $\hat{y}(t)$ по θ.

Для моделей, которые не могут быть описаны как линейные регрессии не возможно точно вычислить предсказатель и его градиент для текущей оценки $\theta(t-1)$. В этом случае используются приближения $\hat{y}(t)$ и $\psi(t)$.

Рассмотрим взвешенный квадратичный критерий ошибки предсказания:

$$V_t(\theta, Z^t) = \gamma(t)\frac{1}{2}\sum_{k=1}^{t}\beta(t,k)e^2(k,\theta) \tag{5}$$

с β и γ, задаваемыми выражениями:

$$\beta(t,k) = \lambda(t)\beta(t-1,k),\ 1 \le k \le t-1,\ \beta(t,t) = 1, \tag{6}$$

где $\lambda(t)$ – коэффициент забывания,

$$\gamma(t) = \left[\sum_{k=1}^{t}\beta(t,k)\right]^{-1}. \tag{7}$$

Функция $V_t(\theta, Z^t)$ для набора данных Z^t является корректно определенной скалярнозначной функцией вектора параметров θ. Она представляет собой естественную меру правильности модели.

Причем

$$\sum_{k=1}^{t}\gamma(t)\beta(t,k) = 1,$$

и градиент по θ имеет вид

$$V_t'(\theta, Z^t) = -\gamma(t)\sum_{k=1}^{t}\beta(t,k)\psi(k,\theta)e^2(k,\theta) =$$

$$= \gamma(t)\left[\lambda(t)\frac{1}{\gamma(t-1)}V_{t-1}'(\theta, Z^{t-1}) - \psi(t,\theta)e(t,\theta)\right] = \quad (8)$$

$$= V_{t-1}'(\theta, Z^{t-1}) + \gamma(t)\left[-\psi(t,\theta)e(t,\theta) - V_{t-1}'(\theta, Z^{t-1})\right].$$

При оценивании на основе метода ошибки предсказания поисковый алгоритм имеет общий вид:

$$\hat{\theta}_t^{(i)} = \hat{\theta}_t^{(i-1)} - \mu_t^{(i)}\left[R_t^{(i)}\right]^{-1} V_t'\left(\hat{\theta}_t^{(i-1)}, Z^t\right). \quad (9)$$

Здесь индекс t означает, что оценка основана на t данных (то есть на Z^t); верхний индекс (i) обозначает i-ю итерацию процедуры минимизации; $R_t^{(i)}$ $d \times d$ – матрица, изменяющая направление поиска; $\mu_t^{(i)}$ – размер шага.

Если на каждой итерации i производиться еще одно измерение данных, то алгоритм можно записать в виде:

$$\hat{\theta}_t^{(t)} = \hat{\theta}_{t-1}^{(t-1)} - \mu_t^{(t)}\left[R_t^{(t)}\right]^{-1} V_t'\left(\hat{\theta}_{t-1}^{(t-1)}, Z^t\right). \quad (10)$$

Для упрощения обозначений введем

$$\hat{\theta}(t) = \hat{\theta}_t^{(t)},\ R(t) = R_t^{(t)}. \quad (11)$$

Предположим, что $\hat{\theta}(t-1)$ действительно минимизирует $V_{t-1}(\theta, Z^{t-1})$, и

$$V_{t-1}'\left(\hat{\theta}(t-1), Z^{t-1}\right) = 0. \quad (12)$$

Тогда из (9) имеем

$$V_t'\left(\hat{\theta}(t-1), Z^t\right) = -\gamma(t)\psi\left(t, \hat{\theta}(t-1)\right)e\left(t, \hat{\theta}(t-1)\right). \quad (13)$$

Используя эту аппроксимацию (и выбирая $\mu(t) = 1$) можно записать следующий алгоритм:

$$\hat{\theta}(t) = \hat{\theta}(t-1) + \gamma(t)R^{-1}(t)\psi\left(t, \hat{\theta}(t-1)\right)e\left(t, \hat{\theta}(t-1)\right). \quad (14)$$

Переменные $\psi\left(t, \hat{\theta}(t-1)\right)$ и $e\left(t, \hat{\theta}(t-1)\right)$ выводятся из выражения для предсказания $\hat{y}\left(t, \hat{\theta}(t-1)\right)$. В общем случае вычисление $\hat{y}(t \mid \theta)$ для произвольного заданного значения θ требует знания всей последовательности

данных Z^{t-1}. Для конечномерных линейных моделей это означает, что $\hat{y}(t \mid \theta)$ образуется на выходе линейного фильтра, коэффициенты которого зависят от θ. Отсюда следует, что $\psi\left(t, \hat{\theta}(t-1)\right)$ и $\hat{y}\left(t, \hat{\theta}(t-1)\right)$ не могут быть вычислены «рекуррентно» (то есть при фиксированной длине памяти). Это приводит к необходимости использования некоторой аппроксимации указанных переменных: на каждом шаге рекуррентного определения $\psi(t, \theta)$ и $\hat{y}(t \mid \theta)$ по Z^t для произвольного заданного θ заменяется, в момент k, параметр имеющейся текущей оценкой $\hat{\theta}(k)$. Полученные приближения величин $\psi\left(t, \hat{\theta}(t-1)\right)$ и $\hat{y}\left(t, \hat{\theta}(t-1)\right)$ обозначим $\psi(t)$ и $\hat{y}(t)$.

Для конечномерной линейной стационарной модели аппроксимацию можно представить в следующем виде:

$$\xi(t+1) = A\left(\hat{\theta}(t)\right)\xi(t) + B\left(\hat{\theta}(t)\right)z(t), \tag{15а}$$

$$\begin{bmatrix} \hat{y}(t) \\ \psi(t) \end{bmatrix} = C\left(\hat{\theta}(t-1)\right)\xi(t), \tag{15б}$$

где $A\left(\hat{\theta}(t)\right)$, $B\left(\hat{\theta}(t)\right)$, $C\left(\hat{\theta}(t-1)\right)$ – некоторые матрицы.

$R(t)$ вычисляется следующим образом:

$$R(t) = \gamma(t)\sum_{k=1}^{t}\beta(t,k)\psi(k)\psi^T(k). \tag{16}$$

Используя в (10) соотношение (13) получим следующую схему:

$$e(t) = y(t) - \hat{y}(t), \tag{17а}$$

$$\hat{\theta}(t) = \hat{\theta}(t-1) + \gamma(t)R^{-1}(t)\psi(t)e(t), \tag{17б}$$

$$R(t) = R(t-1) + \gamma(t)\left[\psi(t)\psi^T(t) - R(t-1)\right], \tag{17в}$$

где $\hat{\theta}(t)$ – оценка параметров во время t.

Схема (17) совместно с (15) представляет собой рекуррентный алгоритм Гаусса–Ньютона метода ошибки предсказания.

В зависимости от выбора $R(t)$ схема (14б) соответствует специальным типам алгоритмов, принадлежащих к широкому семейству рекуррентных методов ошибки предсказания. Например, для линейной регрессии

$$\hat{y}(t \mid \theta) = \varphi^T(t)\theta$$

имеем $\psi(t,\theta) = \psi(t) = \varphi(t)$, и (17) превращается в рекуррентный метод наименьших квадратов.

ЛИТЕРАТУРА:

1. Льюнг Л. Идентификация систем. Теория для пользователя: Пер. с англ./ Под ред. Я.З. Ципкина. – М.: Наука, Гл. ред. Физ.-мат. Лит., 1991.
2. Методы робастного, нейро-нечеткого и аддитивного управления. – М.: МГТУ им. Н.Э. Баумана, 2001. – 744 с., ил. /Под ред. Н.Д. Егупова. (Методы теории автоматического управления).

Получено 10.12.2004. Опубликовано в Internet 20.12.2004. .

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С.94-98. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/021)

ТЕСТИРОВАНИЕ ВЫСОКОНАДЕЖНОЙ БИОМЕТРИИ

Малыгина Е.А., Олейник Ю.И., Малыгин А.Ю.
Пензенский государственный университет,
Пензенский артиллерийский инженерный институт

Проблема обеспечения безопасности информационных технологий занимает все более значительное место в реализации компьютерных систем и сетей. Одним из путей решения данной проблемы является использование биометрико-нейросетевых технологий.

Столь значительное общественное внимание к биометрии привело к тому, что Международная организация по стандартизации (ISO) в лице ее 27-го подкомитета официально рассматривает усиление паролей и персональных кодов биометрией как одну из основных тенденций развития систем информационной безопасности [*www.din.de/ni/sc27*].

Сложившаяся структура объединения усилий правительства США, общественности, фирм производителей биометрии, исследовательских и образовательных организаций отражена в левой части рисунка 1. Соединенные Штаты на данный момент смогли дальше всех пройти по пути национальной стандартизации биометрических устройств и технологий. В этой работе задействованы национальные институты стандартизации США NIST (National Institute of Standards and Technology) и ANSI (American National Standards Institute). Их совместные усилия привели к тому, что на данный момент в США выпущено порядка 15 национальных биометрических стандартов, часть

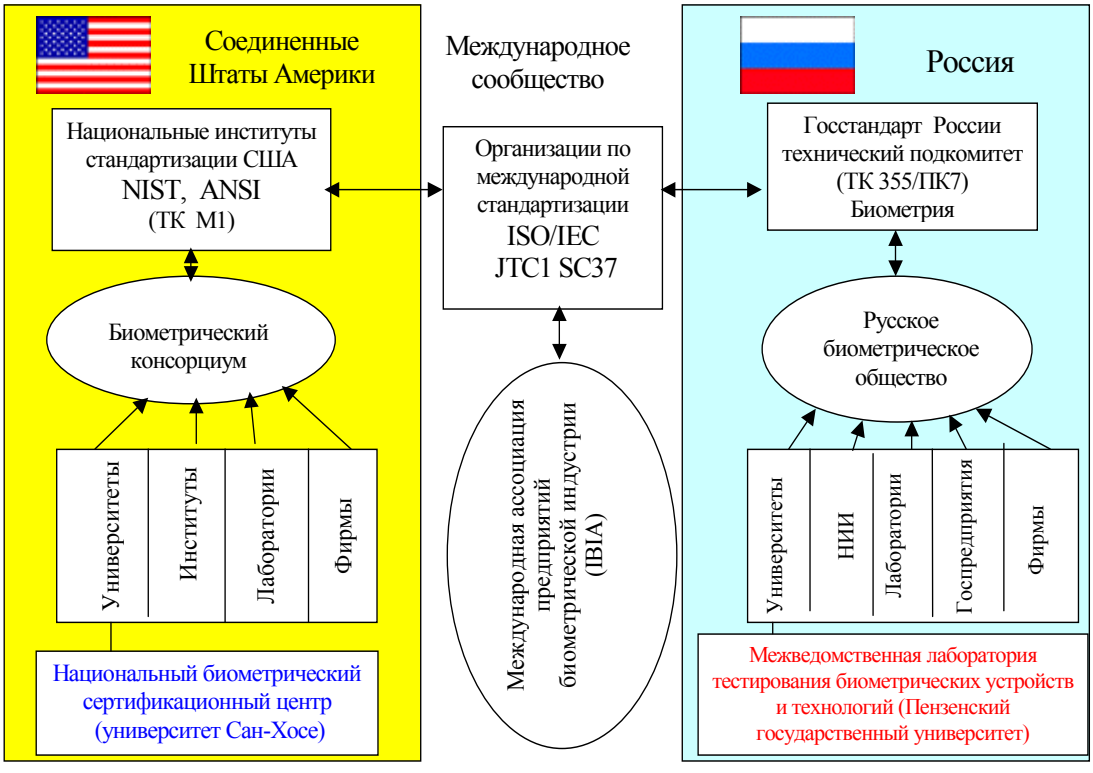


Рисунок 1. Структура организации сотрудничества в области международной и национальной стандартизации

из которых с высокой вероятностью в ближайшем будущем получат статус международных стандартов. Для разработки национальных биометрических стандартов при институтах стандартизации США создан специальный технический комитет M1 основной задачей которого является ускоренная разработка национальных и международных биометрических стандартов [1].

В Соединенных Штатах уже сложилась достаточно устойчивая структура связей объединяющих все биометрическое сообщество. Биометрическая общественность объединена в рамках «Биометрического консорциума» [*www.biometric.org*], организуются ежегодные специализированные биометрические конференции, организован специальный институт биометрии и биометрический центр тестирования при университете города Сан-Хосе (Калифорния, Силиконовая долина), где одновременно готовятся и специалисты по биометрии.

Производители биометрических устройств и технологий объединены в рамках международной ассоциации IBIA (International Biometric Industry Association), которая активно влияет на процессы подготовки новых стандартов. Через IBIA производители регистрируют свои форматы представления биометрические данных, которые далее гармонизируются и обобщаются в виде международных стандартов и рекомендаций. На данный момент зарегистрировано 27 форматов данных, используемых в биометрических устройствах и технологиях различных компаний.

Естественно, что Россия не может оставаться в стороне от наметившихся процессов объединения международных усилий и стандартизации биометрических технологий. Россия в лице Госстандарта является полноправным членом ISO/IEC, в феврале 2003 г. при ГОСТ Р ТК355 (технический комитет «Автоматическая идентификация») был создан 7 подкомитет, занимающийся только вопросами биометрической идентификации. На ГОСТ Р ТК355/ПК7 видимо ляжет вся тяжесть работы по переводу готовящихся международных биометрических стандартов на русский язык и их гармонизации. В настоящий момент ГОСТ Р ТК355/ПК7 в основном состоит из предприятий-членов «Русского биометрического общества». В целом в России получается примерно такая же структура связей биометрической общественности, что и в США (рисунок 2). Отличие этих близких друг другу структур состоит только в масштабах инвестиций и некотором отставании России по времени создания элементов этой структуры. Будем надеяться, что это отставание временно и будет ликвидировано. По крайней мере, все это должно относиться к электронным биометрическим паспортам. Мы не имеем права отставать в этих вопросах и должны в отведенное время решить эту проблему.

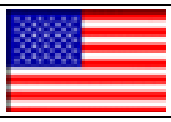
Создание новых биометрических систем ставит задачу тестирования надежности созданных систем. Затрачивая значительные средства на создание, сертификацию и функционирование новых систем с использованием биометрии, общество должно быть уверено, что затраченные средства оправдывают поставленные цели. В связи с этим вопросы тестирования биометрических систем зарубежного и отечественного производства выдвигаются на первый план. В таблице 1 представлены основные биометрические технологии, применяемые в настоящее время.

Из таблицы 1 видно, что технологии биометрического распознавания, разработанные в США и России, находятся практически на одном уровне, за исключением почерка и голоса. Это несоответствие связано не только в отличиях начертания знаков латиницы и кириллицы и произношении фраз на английском и русском языках, но и в принципиальных отличиях создания технологий распознавания.

При этом первые четыре технологии распознавания (таблица 1) дороги в реализации и имеют весьма ограниченные возможности по эффективности. Последние две технологии дешевле в реализации, поэтому развитие технологий биометрического распознавания почерка и голоса более приемлены России. За развитие и более широкое применение технологий распознавания почерка и голоса выступает и то, что в нашу жизнь активно внедряются новейшие средства телекоммуникаций и допуск к их информационным ресурсам посредством голоса и почерка владельца один из оптимальных путей.

Таблица 1

Надежность основных биометрических технологий распознавания

Технология биометрического распознавания	США 	Россия 
	Вероятность пропуска «Чужого»	Вероятность пропуска «Чужого»
Сосуды глазного дна	10^{-8}	10^{-8}
Радужная оболочка глаза	10^{-9}	10^{-9}
Отпечаток пальца	10^{-6}	10^{-6}
Геометрия лица	10^{-2}	10^{-2}
Почерк (слово из 5 букв)	10^{-2}	10^{-22}
Голос (фраза из 3 слов)	10^{-2}	10^{-16}

Однако, уникальность открытых рукописных образов не велика по сравнению с отпечатками пальцев или радужной оболочкой глаза. Повышение стойкости рукописного биометрического образа можно решить с помощью искусственных многослойный нейронных сетей. Многослойные нейросети позволяют преобразовать размытый, нечеткий рукописный образ в однозначный личный ключ пользователя [2]. Обученная большая расширяющаяся нейронная сеть имеет криптографические характеристики по числу возможных комбинаций входных и выходных образов.

Но при разработке новых нейросетевых технологий возникает ряд вопросов, на которых хочется остановиться отдельно.

Одна из них стойкость биометрической системы. Сегодня производителями декларируются только среднестатистические показатели стойкости биометрической системы, что явно недостаточно. Реальные характеристики биометрических систем при работе с конкретными пользователями могут отличаться от среднестатистических на десятки порядков. Необходима разработка механизмов прогноза стойкости реальных биометрических образов, принадлежащих реальным людям. В настоящее время стойкость нейросистем в основном рассчитана с помощью математических моделей на ПЭВМ и с использованием минимального количества биометрических образов реальных людей.

Причина этого кроется в определенных сложностях сбора, обработки, систематизации и использования собранных данных для проверки существующих и разрабатываемых биометрических систем.

В стенах Пензенского государственного университета более семи проводятся работы по созданию и исследованию биометрических технологий. Университет имеет прочные связи с разработчиками и производителями биометрических устройств и технологий. За истекший период в вузе накоплен определенный методический опыт тестирования биометрических устройств и в 2004 году при факультете военного обучения создана межведомственная лаборатория тестирования биометрических устройств и технологий. Целью

лаборатории стало обеспечение сбора, обобщения и систематизации биометрических данных, разработка и совершенствование существующих методик по биометрическим исследованиям, тестирование биометрических устройств и технологий, разрабатываемых и используемых предприятиями и организациями РФ.

За внешней простотой сбора рукописных образов кроется кропотливая работа по разработке и совершенствованию методик, программного и инструментального обеспечения. Использование относительно недорогих планшетов Genius Pen 5x4 с достаточно высоким разрешением и поддержкой 1024 градаций степени нажатия пера позволяет снимать трехмерные характеристики почерка.

В среднем на одного респондента затрачивается 50 минут. В этот временной интервал включается момент ознакомления с планшетом и пером, программой «Нейрокриптон» (ПНИЭИ), особенностью написания слов с использованием планшета, сбор, запоминание и обработка 20 образов.

Каждый из пользователей, входящих в тестовую группу, должен находиться в нормальном психологическом состоянии (отсутствие стресса), а так же быть лояльным к тестируемой биометрической системе. Умение пользоваться системой и психологическое состояние контролируется руководителем эксперимента до проведения эксперимента.

В ходе проведения эксперимента с помощью программы «Нейрокриптон», ее обработки показали, что всех людей можно разделить на 7 классов [3]. Каждый класс имеет свою уникальность почерка, стабильность почерка. Меняя парольные слова можно переходить из одного класса в другой. Вполне реально перейти на один класс ниже или выше, однако переход на 2 класса вверх и вниз возможен, но проблематичен. Стойкость системы к атакам подбора существенно зависит от класса, к которому система отнесла пользователя. Таким образом, стойкость системы во многом определяется индивидуальными характеристиками самого пользователя (его классом). Для практики крайне важно точно определить класс пользователя. Ошибка в определении класса может привести к завышению или занижению стойкости системы на несколько порядков. Поэтому необходимо использовать специальные нейросетевые механизмы для корректного и достоверного определения класса пользователя по его реальным биометрическим параметрам. Тем не менее, как показывает практика, системы динамической биометрии оказываются эффективными длительное время. Существующие данные свидетельствуют о стабильном сохранении отработанных двигательных навыков у человека в течение нескольких десятилетий.

Для проверки высоконадежных биометрических систем количество образов должно быть выше или, в крайнем случае, сопоставимо с заявленной степенью стойкости. Отсюда встает наиболее сложный вопрос создания больших биометрических баз. При всех благоприятных условиях создание необходимых баз для проверки заявленной стойкости почерка (таблица 1) потребует нескольких лет кропотливой работы. Применение зарубежных баз для тестирования данных технологий неприемлемо по указанным выше причинам.

Дальнейший рост надежности биометрии почерка практически реализуем, что нельзя сказать об адекватном росте необходимых для проверки баз.

Закономерно встает вопрос решения данной проблемы. Один из путей – создание специализированной программы, позволяющей путем модификации существующих баз получать новые биометрические образы.

В связи с расширением области применения биометрических технологий встает еще один немаловажный вопрос подготовки дипломированных

специалистов в данной области. Прообразом может послужить подготовка специалистов в университете Сан-Хосе (США).

ЛИТЕРАТУРА:

1. Гермогенов А.П. ФСБ России: государственный подход к созданию идентификационных систем. «ИФОФОРУМ» журнал «Бизнес и Безопасность в России» 2005 г., № 40, январь 2005, стр.32–42.
2. Волчихин В.И., Иванов А.И. Биометрия: быстрое обучение искусственных нейронных сетей. Пенза: изд-во Пензенского государственного университета, 2000.
3. Иванов А.И., Петруненков А.А. Развитие биометрических технологий: объединение усилий и переход к этапу стандартизации. Журнал «Современные технологии безопасности» №3, 2004.

Материалы поступили 20.12.2004. Опубликовано в Internet 20.12.2004. .

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С. 99-104. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/022)

АТАКИ НА ПРОТОКОЛЫ УСТАНОВЛЕНИЯ КЛЮЧА

Давыдов А.Н.
НПФ «Кристалл»

Введение

Исследование успешно реализованных атак на протоколы установления ключа позволяет обнаруживать недостатки в существующих протоколах, учитывать прежние ошибки разработки, понимать методы и стратегии атак и определять принципы разработки. В данной статье приводятся описания атак на протоколы установления ключа и даются методы защиты от каждой группы атак.

Обозначения

В данной статье приняты следующие обозначения:

E<*key*>(*text*)	–	шифрование данных *text* на ключе *key* по симметричному алгоритму;
D<*key*>(*chtext*)	–	расшифрование данных *chtext* на ключе *key* по симметричному алгоритму;
SK<key_p>(*text*)	–	вычисление цифровой подписи от данных *text* на ключе key_p;
VK<key_o>(*text*)?(*sign*)	–	проверка цифровой подписи *sign* от данных *text* на ключе key_o;
EK<key_o>(*text*)	–	шифрование данных *text* на ключе key_o по асимметричному алгоритму;
DK<key_p>(*chtext*)	–	расшифрование данных *chtext* на ключе key_p по асимметричному алгоритму;
A, *B*	–	участники протокола;
E	–	злоумышленник;
T	–	третья доверенная сторона;
A → *B*: *S*	–	участник *A* передаёт участнику *B* сообщение *S*;
E(«*A*»)	–	злоумышленник *E* от лица участника *A*;
X, *Y*	–	операция конкатенации строк *X* и *Y*.

Атака повтора сообщений

Злоумышленник предварительно сохраняет старые сообщения, которыми легальные участники протокола обмениваются в предыдущих сеансах выполнения протокола. Злоумышленник атакует протокол, повторяя предварительно сохранённое старое сообщение в текущем сеансе протокола. Общей целью протоколов аутентификации является определение активного соответствия участников протокола. Достижение данной цели в общем случае достигается путём обмена свежими сообщениями между участниками. Повтор старых сообщений не позволяет протоколу аутентификации достигнуть своей цели.

Повтор сообщения – это классическая атака на протоколы аутентификации и протоколы аутентифицированного установления ключа. Атаку повтора сообщений можно обнаружить посредством повсеместного использования идентификаторов свежести (нонсов, отметок времени). Но следует заметить, что иногда криптографическое связывание идентификатора свежести и сообщения только указывает на свежесть выполнения операции криптографического

объединения, но не указывает на свежесть объединяемого сообщения. В [1] приводится следующий пример атаки повтора сообщений. Пользователь A имеет симметричный ключ K_{AT} общий с сервером аутентификации T. Пользователь A хочет получить ключ K_{AB} для установления безопасной связи с пользователем B. Он посылает отметку времени T_A. B вычисляет $E<K_{AB}>(T_A+1)$ и возвращает:

$B \rightarrow A$: $B, A, E<K_{AB}>(T_A+1), E<K_{AT}>(K_{AB})$.

Таким образом, хотя идентификатор свежести и криптографически объединён с ключом K_{AB}, пользователь A не может убедиться, что K_{AB} является свежим. Он может убедиться только в том, что ключ K_{AB} использовался недавно, но он может быть старым или даже скомпрометированным.

Атака «человек посередине»

Атака «человек посередине» применима к коммуникационным протоколам, в которых отсутствует взаимная аутентификация сторон. Для реализации такой атаки злоумышленник передаёт условие сложной задачи, ответ на которую один участник протокола спрашивает у другого участника, а затем возвращает ответ (возможно, после простой обработки) назад запрашивающей стороне и/или наоборот. В качестве сложных задач, как правило, используются задача разложения на простые множители (задача об укладке ранца) и задача дискретного логарифмирования.

Классическая атака «человек посередине» на протокол неаутентифицированного соглашение ключа Диффи-Хеллмана выполняется следующим образом.

$A \rightarrow E(«B»)$: α^x; (1)

$E(«B») \rightarrow B$: $\alpha^{x'}$; (1′)

$B \rightarrow E(«A»)$: α^y; (2)

$E(«A») \rightarrow A$: $\alpha^{y'}$. (2′)

A и B имеют закрытые ключи x и y, соответственно. α – несекретное простое число, известное A и B. Злоумышленник E создаёт ключи x' и y'. E перехватывает экспоненту A и заменяет её на $\alpha^{x'}$; перехватывает экспоненту B и заменяет её на $\alpha^{y'}$. A формирует сеансовый ключ $K_A = \alpha^{xy'}$, тогда как B формирует сеансовый ключ $K_B = \alpha^{x'y}$. E может вычислить оба этих ключа. Когда A посылает B сообщение, шифрованное на K_A, E расшифровывает его, перешифровывает на K_B, и передаёт B. Аналогично E расшифровывает сообщения шифрованные B (для A) на K_B, и перешифровывает их на K_A. A и B думают, что между ними установлено безопасное соединение, тогда как E читает весь трафик.

Для защиты от атаки «человек посередине» нужно обеспечить аутентификацию источника данных в обоих направлениях обмена сообщениями [2].

Атака с использованием параллельного сеанса

В атаке с использованием параллельного сеанса под управлением злоумышленника одновременно выполняются два или более сеансов протокола. Параллельное выполнение позволяет злоумышленнику получить ответ на сложную задачу в одном из управляемых им сеансов, а затем использовать ответ в другом сеансе. В атаке с использованием параллельного сеанса предполагается, что последовательность сеансов не важна.

Предположим, что A и B имеют общий симметричный ключ K_{AB}, и аутентифицируют друг друга на основе предъявления знания этого ключа посредством шифрования или расшифрования нонсов N_A и N_B.

$A \rightarrow B$: N_A; (1)

$B \rightarrow A$: $E<K_{AB}>(N_A, N_B)$; (2)

$A \rightarrow B$: N_B. (3)

Злоумышленник E может выдать себя за B следующим образом. E перехватывает сообщение (1), и начинает выполнять новый протокол, посылая назад A идентичное сообщение N_A как сообщение (1) подразумеваемое от B. Во втором протоколе A отвечает сообщением (2′) $\mathrm{E}<K_{AB}>(N_A, N'_A)$, которое E снова перехватывает и просто возвращает назад A в качестве ответа (2) на запрос N_A в первом протоколе. После этого A завершает первый протокол, и верит, что он успешно аутентифицировал B, тогда как на самом деле B не участвовал ни в каких обменах информацией.

$A \rightarrow E(«B»)$: N_A; (1)
$E(«B») \rightarrow A$: N_A; (1′)
$A \rightarrow E(«B»)$: $\mathrm{E}<K_{AB}>(N_A, N'_A)$; (2′)
$E(«B») \rightarrow A$: $\mathrm{E}<K_{AB}>(N_A, N_B = N'_A)$; (2)
$A \rightarrow E(«B»)$: N_B. (3)

Для обнаружения атак с использованием параллельного сеанса следует контролировать аутентичность источника сообщений путём криптографического связывания сообщения с идентификатором его источника и аутентичность сообщений протокола с помощью нонсов или номеров сообщений. Для аутентификации следует использовать хеширование, а не шифрование.

Атака отражения сообщений

В атаке отражения, когда честный участник протокола посылает сообщение другому участнику, злоумышленник перехватывает сообщение и посылает его назад отправителю. Злоумышленник может изменять идентификационную и адресную информацию в соответствии с правилами низкоуровневого коммуникационного протокола так, что создатель сообщения и не заметит, что отражённое сообщение было создано им самим.

В атаке отражения злоумышленник пытается заставить поверить создателя сообщения, что отражённое сообщение создано для него участником протокола. Если действия злоумышленника успешны, то создатель сообщения принимает ответ на запрос, на который на самом деле он ответил сам.

Для защиты от атак отражения следует избегать симметрии в сообщениях. Избежать симметрии в сообщениях возможно не только путём использования сообщений с различной структурой, но и, например, путём использования различных ключей для шифрования сообщений, передаваемых от A к B и от B к A.

Атака чередования

Атака чередования представляет собой комбинацию атак с использованием параллельного сеанса и атак отражения. В качестве примера рассмотрим следующий протокол. Предположим, что стороны A и B имеют собственные закрытые ключи подписи PK_A и PK_B, соответственно, и аутентичные копии открытых ключей друг друга.

$A \rightarrow B$: N_A; (1)
$B \rightarrow A$: N_B, $\mathrm{SK}<PK_B>(N_B, N_A, A)$; (2)
$A \rightarrow B$: N'_A, $\mathrm{SK}<PK_A>(N'_A, N_B, B)$. (3)

Идея данного протокола заключается в том, что случайные числа N_A и N_B, выбираемые A и B, соответственно, вместе с подписями предоставляют гарантию свежести и аутентификации объекта. Однако, злоумышленник E может начать выполнение одного протокола с B (выдавая себя за A) и другого протокола с A (выдавая себя за B) как показано ниже, и использовать сообщение из последнего протокола, чтобы успешно закончить первый, таким образом заставляя B поверить, что E является A (и что A начал выполнять протокол).

$E(«A») \rightarrow B$: N_A; (1)
$B \rightarrow E(«A»)$: N_B, $\mathrm{SK}<PK_B>(N_B, N_A, A)$; (2)

$E(«B») \rightarrow A$: N_B; (1′)
$A \rightarrow E(«B»)$: N'_A, SK<PK_A>(N'_A, N_B, B); (2′)
$E(«A») \rightarrow B$: N'_A, SK<PK_A>(N'_A, N_B, B). (3)

Данная атака возможна из-за симметрии сообщений (2) и (3), и её можно предотвратить посредством различного формата этих структур, добавляя идентификатор, указывающий номер сообщения, в каждое сообщение, или просто требуя, чтобы исходное N_A заменило N'_A в сообщении (3).

Атака, обусловленная дефектом типов данных

Атака, обусловленная дефектом типов данных, основана на уязвимости, заключающейся в том, что пользователь не может связать сообщение или компонент сообщения с его семантическим значением. При успешно проведённой атаке, обусловленной дефектом типов данных, честный участник протокола ошибочно принимает нонс, отметку времени или идентификатор за ключ. Атака такого типа возможна, когда информация о типах компонентов сообщения явно не определена. Рассмотрим следующий протокол [3]. Участники A и B имеют симметричные ключи, общие с третьей доверенной стороной T, K_{AT} и K_{BT}, соответственно.

$A \rightarrow B$: A, N_A; (1)
$B \rightarrow T$: E<K_{BT}>(A, N_A, T_B), N_B; (2)
$T \rightarrow A$: E<K_{AT}>(B, N_A, K_{AB}, T_B), E<K_{BT}>(A, K_{AB}, T_B), N_B; (3)
$A \rightarrow B$: E<K_{BT}>(A, K_{AB}, T_B), E<K_{AB}>(N_B). (4)

Заявленной целью этого протокола является обеспечение взаимной аутентификации участников протокола A и B и аутентифицированное установление ключа K_{AB}, используя доверенную третью сторону T. Если нонс N_A и ключ K_{AB} имеют один и тот же размер, то ключ не защищён от атаки, обусловленной дефектом типов данных.

$E(«A») \rightarrow B$: A, N_A; (1)
$B \rightarrow E(«T»)$: E<K_{BT}>(A, N_A, T_B), N_B; (2)
нет обмена сообщениями; (3)
$E(«A») \rightarrow B$: E<K_{BT}>(A, N_A, T_B), E<N_A>(N_B). (4)

Злоумышленник использует нонс N_A вместо ключа K_{AB}. Участник протокола B не заметит подмены, если он не может различать типы данных.

Дефект типов данных обычно зависит от реализации. Если спецификация протокола в явном виде не описывает типы данных, используемые в протоколе, то высока вероятность дефекта типов в реализациях.

Атака, обусловленная отсутствием именования

Часто в протоколах аутентификации имена, относящиеся к сообщению, могут быть получены из других элементов данных контекста. Однако если информация об именах не может быть получена из других элементов данных, отсутствие имени может привести к серьезным последствиям. Зачастую разработчики протоколов, желая получить изящный протокол, содержащий минимальную избыточность, склонны опускать имена. Для иллюстрации вышесказанного рассмотрим протокол Деннинг–Сакко [4]. Целью данного протокола является установление общего ключа сторонами A и B, используя доверенную третью сторону T. $Cert_A$ и $Cert_B$, соответственно, обозначают результат криптографического связывания открытых ключей участников A и B и их идентификаторов.

$A \rightarrow T$: A, B; (1)
$T \rightarrow A$: $Cert_A$, $Cert_B$; (2)
$A \rightarrow B$: $Cert_A$, $Cert_B$, EK<OK_B>(K_{AB}, T_A, SK<PK_A>(K_{AB}, T_A)). (3)

В этом протоколе обеспечивается конфиденциальность и подлинность сообщения 3. Когда участник B получает сообщение от участника A, он предполагает, что сеансовый ключ K_{AB} является разделяемым между ним и участником A, потому что сообщение 3 содержит подпись участника A, и для его создания использовался открытый ключ участника B.

Но данный протокол не гарантирует единственность разделения ключа. Участник протокола B после получения сообщения 3 может обмануть другого пользователя:

$B(«A») \rightarrow C$: $Cert_A, Cert_C, \mathrm{EK}<OK_C>(K_{AB}, T_A, \mathrm{SK}<PK_A>(K_{AB}, T_A))$. (3')

Пользователь C, получив данное сообщение, предполагает, что отправителем сообщения является A. Если C пошлёт A конфиденциальное сообщение, то B сможет прочесть его. Чтобы защититься от такой атаки сообщение 3 протокола должно выглядеть следующим образом:

$A \rightarrow B$: $Cert_A, Cert_B, \mathrm{EK}<OK_B>(A, B, K_{AB}, T_A, \mathrm{SK}<PK_A>(A, B, K_{AB}, T_A))$.(3)

Для защиты от атак, обусловленных отсутствием именования, при разработке протоколов нужно придерживаться правила, что если подлинность участника протокола важна для смыслового содержания сообщения, то имя пользователя следует явно указать в сообщении.

Атака, обусловленная неправильным использованием криптографических служб

Неправильное использование криптографических служб может повлечь за собой различные атаки. Для примера рассмотрим проведение атаки на протокол Отвея-Рииса [5]. Протокол Отвея-Рииса включает следующие сообщения:

$A \rightarrow B$: $M, A, B, \mathrm{E}<K_{AT}>(N_A, M, A, B)$; (1)

$B \rightarrow T$: $M, A, B, \mathrm{E}<K_{AT}>(N_A, M, A, B), \mathrm{E}<K_{BT}>(N_B, M, A, B)$; (2)

$T \rightarrow B$: $\mathrm{E}<K_{AT}>(N_A, K), \mathrm{E}<K_{BT}>(N_B, K)$; (3)

$B \rightarrow A$: $\mathrm{E}<K_{AT}>(N_A, K)$. (4)

После получения сообщения (2), третья доверенная сторона T должна проверить, что шифрованные поля (M, A, B) в обеих частях сообщения совпадают друг с другом, и что эти поля соответствуют открытому тексту (M, A, B). Если не выполняется последняя проверка, то протокол подвержен атаке злоумышленника E, который является авторизованным пользователем системы, выдающим себя за B следующим образом. E изменяет сообщение (2), заменяя открытый текст B на свой открытый текст, но оставляя неизменными оба идентификатора и A, и B в обоих шифротекстах, заменяя нонс N_B на свой нонс N_E, и используя ключ K_{ET} который до выполнения протокола является общим для A и T вместо K_{BT}. Основываясь на идентификаторе E из открытого текста, T шифрует часть сообщения (3) на ключе K_{ET}, позволяя E получить K; но A верит, как в неизмененном протоколе, что ключ K является общим с B.

$A \rightarrow B$: $M, A, B, \mathrm{E}<K_{AT}>(N_A, M, A, B)$; (1)

$B \rightarrow E(«T»)$: $M, A, B, \mathrm{E}<K_{AT}>(N_A, M, A, B), \mathrm{E}<K_{BT}>(N_B, M, A, B)$; (2)

$E(«B») \rightarrow T$: $M, A, E, \mathrm{E}<K_{AT}>(N_A, M, A, B), \mathrm{E}<K_{ET}>(N_E, M, A, B)$; (2′)

$E \leftarrow T$: $\mathrm{E}<K_{AT}>(N_A, K), \mathrm{E}<K_{ET}>(N_E, K)$; (3)

$A \leftarrow E$: $\mathrm{E}<K_{AT}>(N_A, K)$. (4)

Атака возможна из-за слабости способа, с помощью которого A определяет идентичность стороны, предоставившей K в сообщении (4). Участник A не может точно определить, кому T предоставил K. Участник A надеется на связь нонса N_A в сообщении (4) с (N_A, B) в защищенной части сообщения (1). Таким образом, A надеется, что T предоставит K только той стороне, которой она запросила, но это можно гарантировать, только если T использует защищенные поля (M, A, B).

Выводы

1. Не существует универсального метода, позволяющего обезопасить протокол установления ключа от атак всех типов.

2. Необходимо учитывать известные и характерные для данной среды атаки при разработке и анализе протоколов установления ключа.

3. Оптимизацию протокола следует выполнять очень осторожно, чтобы не внести уязвимости в протокол или не изменить заявленные цели протокола.

ЛИТЕРАТУРА:

1. V. Varadharajan, P. Allen, and S. Black. An analysis of the proxy problem in distributed systems. In Proceedings of the 1991 IEEE Symposium on Security and Privacy: pages 255–275, 1991.
2. M. Wenbo. Modern Cryptography: Theory and Practice. Prentice Hall PTR, pages 648, 2003.
3. B.C. Neuman and S.G. Stubblebine. A note on the use of timestamps as nonces. ACM Operating Systems Review, 27(2): pages 10–14, April 1993.
4. D.E. Denning and G.M. Sacco. Timestamps in key distribution protocols. Communications of the ACM, 24(8): pages 533–536, August 1981.
5. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone. Handbook of applied cryptography. CRC Press, pages 816, 1996.

Получено 20.12.2004. Опубликовано в Internet 20.12.2004. .

Труды научно-технической конференции
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Том 5. С. 105-108. Секция-9: Аутентификация: парольная, биометрическая, криптографическая.
Пенза-2004 (http://beda.stup.ac.ru/RV-conf/v05/023)

ВЕРОЯТНОСТНЫЙ ПОДХОД К РАЗДЕЛЕНИЮ ШУМОВЫХ И ДЕТЕРМИНИРОВАННЫХ СОСТАВЛЯЮЩИХ РЕЧЕВОГО СИГНАЛА

Надеев Д.Н., Иванов А.И.
ФГУП «ПНИЭИ»

В настоящее время в России изучается возможность синтеза высоконадежных биометрико-нейросетевых механизмов преобразования тайного рукописного или голосового пароля в тайну личного ключа пользователя. При этом совершенно очевиден тот факт, что для получения высокой надежности нейросетевого преобразования исходные речевые данные должны подвергаться качественной предобработке. Практика показала, что качества обработки речевого сигнала классических вокодеров недостаточно для решения задач высоконадежной речевой биометрии.

Существующие системы преобразования аналогового речевого сигнала в цифровую форму, работа которых построена на методе линейного предсказания, не обеспечивают четкого разграничения тонового и шумового компонент речи. Это практически не сказывается на восприятии восстановленной речи человеком, однако приводит к существенным ошибкам биометрических механизмов. В процессе преобразования каждого речевого кадра (участка речевого сигнала определенной длины) современные вокодеры генерируют код флагов огласованности, по эквивалентному уровню которых выносится решение о типе кадра (тон или шум). Анализ работы этих механизма на ряде примеров показывает, что разделение тон/шум происходит не всегда правильно, наблюдается пропуск кадров с полезной информацией, нестабильность флагов на переходных участках достигает 1…3 кадров. В дальнейшем, использование подобной неопределенности данных при подаче их на входы нейросети снижает качество ее выходных решений.

Подробно описанные в литературе классические алгоритмы цифровой обработки сигналов во временной и частотной областях, построенные с использованием преобразований Фурье, прямого и обратного z-преобразований, а также методы двумерной обработки [1] при кодировании фраз с большим количеством вокализованных и невокализованных кадров дают неоднозначные характеристики на участках смены букв и границах слов и фраз. Одним из подходов к решению задачи повышения качества входных данных нейросети является переход от попыток определения детерминированных границ речевых компонент тон/шум к применению для их описания вероятностных характеристик. Такие величины не предназначены для строгого разграничения сигнала речи по признаку тон/шум, а представляют собой вероятностную меру (в пределах от 0 до 1), дающую представление о том, какую долю в данном кадре имеет тоновая (детерминированная) и случайная, шумовая составляющие.

Принятие решения в пользу конкретного варианта выполняется по нескольким хорошо известным методикам измерения соотношения тон/шум:

1) по уровню интенсивности звука $\beta_ш$

$$\beta_ш = 10 \lg \frac{I_ш}{I_0}$$

$I_ш$ – сила звука; I_0 – единица силы звука, $I_0 = 10^{-16}\,вт/см^2$ или уровню спектра звука B

$$B = 10\lg\frac{I}{I_0\Delta f_э} = 10\lg\frac{I}{I_0} - 10\lg\Delta f_э,$$

$\Delta f_э$ – численное значение эквивалентной полосы частот, в которой был измерен уровень интенсивности.

2) корреляционным преобразованием, оценивающим периодическую составляющую сигнала

$$\rho = \frac{\mathrm{cov}(X, Xz)}{\delta_X \delta_{Xz}},$$

$$\mathrm{cov}(X, Xz) = \frac{1}{n}\sum(X_i - \mu_X)(Xz_i - \mu_{Xz}),$$

$$\delta_X = \sqrt{\frac{1}{n}\sum(X_i - \mu_X)^2},$$

$$\delta_{Xz} = \sqrt{\frac{1}{n}\sum(Xz_i - \mu_{Xz})^2}.$$

Здесь X, μ_X, δ_X – исходный вектор отчетов речевого сигнала, его математическое ожидание и разброс; $Xz, \mu_{Xz}, \delta_{Xz}$ – вектор X, взятый с фазовым смещением z и его статистические характеристики его математическое ожидание и разброс; $\mathrm{cov}(X, Xz)$ – коэффициенты ковариации двух векторов.

3) по динамическому диапазону соотношения энергий в полосах частот;
4) по периоду основного тона, например, вычисленному кепстральным преобразованием.

Далее строится нейросетевой выделитель двух образов (тональных образов и шумовых образов) с выходными сигналами пропорциональными расстоянию предъявленного фрагмента речи к первому или второму выделяемому образу. При входных тональных воздействиях выход «тон» нейросети должен иметь единичное или близкое к нему значение. При входных шумовых воздействиях выход «шум» должен иметь единичное или близкое к нему значение.

В качестве иллюстрации работы данного типа нейросетевых механизмов приводятся диаграммы речи, на которых хорошо видны преимущества использования вероятностных мер в отличие от строго детерминированных вокодерных флагов. В реальных звуковых сигналах нет четкого перехода из одного класса (тон) в другой класс (шум). Как следствие создать классификатор тон/шум с корректным выделением и абсолютно детерминированными выходными сигналами невозможно. Пытаясь поднять уровень однозначности выходных решений тон/шум, мы теряем существенную промежуточную информацию.

На рисунке 1 приведен пример неоднозначного выделения слова из звукового сигнала. Эта неоднозначность так же может являться причиной сбоев при нейросетевом распознавании речевых команд и преобразовании паролей в ключ. Как показывает практика, эту неоднозначность можно уменьшить, отказавшись от строго детерминированого подхода к выделению слова на фоне шумовых пауз.

На рисунке 2 показан один из примеров тонового, шумового и промежуточного кадров речевого потока на примере словосочетания «с-е» из слова «семьдесят».

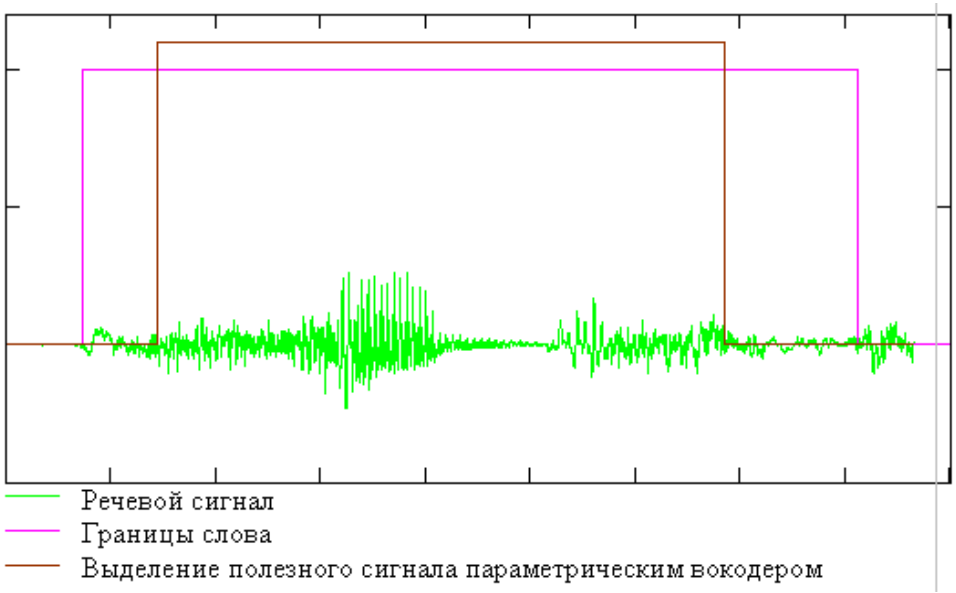


Рисунок 1. Пропуск полезной информации вокодером при разделении речи на отдельные слова.

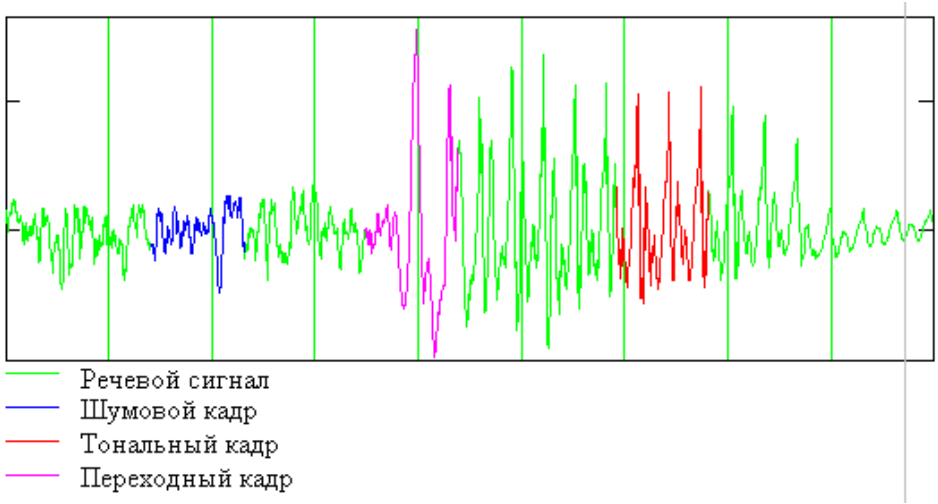


Рисунок 2. Пример тонального, шумового и переходного кадров, содержащихся в речевом потоке (звукосочетание «с-е» из слова «семьдесят»).

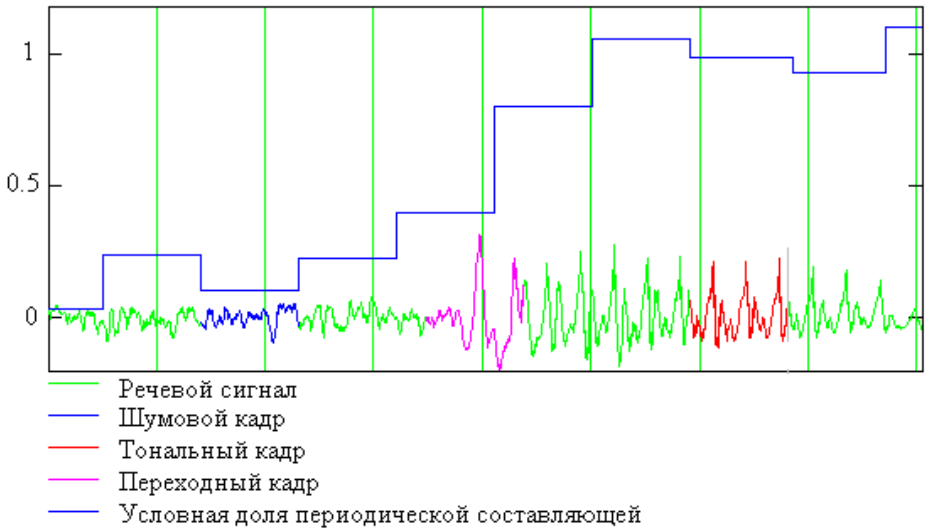
Для обучения и тестирования нейросетевого механизма была создана библиотека тоновых сигналов и шумовых сигналов, вырезанных из речевого потока и преобразованных в векторную форму для удобства последующей их обработки в среде MathCAD. Далее на этих выборках были рассчитаны условные доли содержащейся в них тоновой составляющей, конечные значения вероятностей интерпретации звуковых фрагментов как тона сведены в вектора $v1$, $v2$, $v3$ (см. таблицу 1).

Таблица 1. Вероятности состояния «тон» для трех анализируемых групп кадров

Номера кадров	Явно шумовые, случайные фрагменты	Смешанные фрагменты речи	Явно тоновые (детерминированные) фрагменты
1	0,1	0,49	1,01
2	0,03	0,71	1,03
3	0,19	0,39	0,97
4	0,15	0,45	0,95

5	0,19	0,27	1,05
6	0,14	0,62	0,98
7	0,04	0,38	0,96
8	0,06	0,4	1,02
9	0,03	0,23	1,04
10	0,19	0,36	0,95
11	0,03	0,44	0,96
12	0,05	0,7	0,89
13	0,09	0,68	0,98
14	0,1	0,39	1,04
15	0,08	0,48	1,06
16	0,11	0,55	0,94

По характеру распределений значений в векторах можно с приемлемой для практики достоверностью констатировать наличие 4 классов фонем, которых два являются детерминированными сигналами («Только тон», «Тон + малый шум»), а оставшиеся два класса носят в себе черты шумовой составляющей («Шум + малый тон», «Только шум»). Распределения фонем для этих классов, в отличие от 1 и 4, отличаются большими по величине дисперсиями, и нормальные кривые в значительной мере перекрываются. Это указывает на недостаточность простой бинарной классификации тон/шум. Необходимо вводить новые дополнительные классы, которые будут включать вполне определенные звукосочетания и обладать по отношению друг к другу более различимыми характеристиками. При использовании нейросетевой технологии появляется возможность существенно расширить число выделяемых классов фонем и тем самым повысить достоверность распознавания.



Таким образом, применение вероятностных мер при априорной обработке речевого сигнала на входах нейросетевого автомата может снизить остроту вопроса о некорректности функционирования вокодеров в части разделения ими классов тон/шум, и, как следствие, может стать одним из путей дальнейшего повышения качества распознавания биометрических образов и уменьшения ошибок первого и второго рода нейросетевых командных автоматов.

ЛИТЕРАТУРА:

1. Л. Робинер, Б. Гоулд. Теория и применение цифровой обработки сигналов. М.: «Мир», 1977.

Материалы поступили 20.12.2004. Опубликовано в Internet 20.12.2004.

СОДЕРЖАНИЕ

Труды научно-технической конференция
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Том 5
Пенза – 2004 г.

ЛР № 020779

Подписано к печати 28.04.2005 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