граммного обеспечения для защищенных АС, учитывающей различные аспекты обеспечения безопасности информации на всех этапах разработки.

Предложения ФГУП «Концерн “Системпром”» в части создания перспективных подсистем СЗИ для АС ВН таковы:

Название подсистемы	**Состав и основные функции**
Подсистема обнаружения атак	средства сбора информации о контролируемых параметрах АС; средства обнаружения атак; средства идентификации атак и обучения обнаружению новых атак
Подсистема извлечения и накопления знаний	средства сбора данных о методах и средствах атак, с использованием технологий создания ложных объектов атаки; средства предварительного анализа, структуризации и хранения знаний об уязвимостях АС и атаках
Подсистема анализа защищенности	средства сбора информации о параметрах АС; средства анализа и получения количественных показателей уровня защищенности АС
подсистемы адаптации СЗИ	средства принятия решения для формирования сигналов управления; средства регулирования параметров СЗИ АС
Подсистема активного противодействия атакам	средства выбора оптимальной стратегии противодействия; средства активного воздействия на процесс совершения атаки
Подсистема маскировки сегментов и элементов сети АС ВН	средства скрытия сегментов и элементов сетей АС ВН, с целью нейтрализации воздействия противоборствующей стороны на АС ВН; имитация сегментов и элементов сетей АС ВН, с целью выявления, оценки и прогнозирования угроз Российской Федерации и ее Вооруженным Силам в информационной сфере; дезинформация и демонстративные действия, с целью введения противоборствующей стороны в заблуждение относительно состава, положения, состояния, предназначения и характера деятельности АС ВН

Л.К. Бабенко, В.Г. Захаревич, О.Б. Макаревич
Россия, г. Ростов-на-Дону, Южный федеральный университет
г. Таганрог, Технологический институт ЮФУ

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ РЕАЛИЗАЦИЯ В НАУЧНОЙ И ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ЮЖНОГО ФЕДЕРАЛЬНОГО УНИВЕРСИТЕТА

В докладе рассматриваются некоторые проблемы информационной безопасности и их реализация в рамках учебного процесса на кафедре безопасности информационных технологий ТТИ ЮФУ и при выполнении соответствующих НИ-

ОКР. С одной стороны, преподаватели, студенты, магистранты, аспиранты вовлекаются в реально проводимые кафедрой НИР и ОКР, с другой стороны, результаты научной работы широко используются в учебном процессе. Важно подчеркнуть, что многие из читаемых на кафедре **курсов базируются на собственных разработках.** Практически весь состав преподавателей занимается научной работой, активно участвует в конференциях и семинарах. Некоторые из рассматриваемых в докладе проблем успешно решаются совместно с сотрудниками лаборатории «Фундаментальных проблем информационной безопасности» (ФПИБ), созданной ИИПРУ КБНЦ РАН в 2005 г.

Проблема защиты компьютерной сети от несанкционированных вторжений на сегодня является наиболее актуальной. В последние годы отмечается явная тенденция к увеличению количества атак на информационные системы (ИС). Причин этому несколько. Прежде всего, возросло количество уязвимостей, ежедневно обнаруживаемых в программно-аппаратном обеспечении ИС. Увеличилось и количество возможных объектов атаки. Так, если совсем недавно в качестве основных объектов несанкционированного воздействия рассматривались исключительно серверы стандартных Web-служб (HTTP, SMTP и FTP), то теперь появились средства для атак на маршрутизаторы, коммутаторы, межсетевые экраны и другие компоненты современных ИС. Вследствие этого появилась и необходимость разработки более эффективных инструментов противодействия нарушителям. К таким инструментам относятся системы обнаружения атак (СОА) [1], представляющие собой программно-аппаратные комплексы (рис.1), предназначенные для выявления несанкционированных действий в ИС.

В ходе выполнения исследований сетевых атак и злоупотреблений была разработана оригинальная и эффективная система обнаружения атак. Система использует метод комбинированного поиска, основанный на обнаружении аномалий сетевого трафика, свидетельствующих об атаке, и строковых сигнатур атак (злоупотреблений). Разработанная на кафедре БИТ ТРТУ система обнаружения атак имеет архитектуру «клиент-сервер» и использует искусственные нейронные сети для обнаружения атак. В ней выделяется два основных модуля:

- устройство управления и отображения информации (консоль);
- устройство перехвата сетевого трафика (сенсор).

Большинство современных СОА осуществляют обнаружение атак путём контроля профилей поведения либо поиска специфических строковых сигнатур. Используя эти методы, практически невозможно создать полную базу данных (БД), содержащую сигнатуры большинства атак. Существует три главные причины этого.

1. Новые сигнатуры необходимо создавать вручную. Сигнатуры известных атак, которые уже включены в БД, не могут гарантировать надёжной защиты без постоянных обновлений.
2. Теоретически существует бесконечное число методов и вариантов атак, и для их обнаружения понадобится БД бесконечного размера. Таким образом, имеется возможность того, что некая атака, не включённая в базу данных, может быть успешно осуществлена.
3. Современные методы обнаружения вызывают большое число ложных тревог. Таким образом, могут быть скомпрометированы легальные сетевые события.

Основное преимущество систем обнаружения атак, использующих нейронные сети, в том, что нейросеть не ограничена знаниями, которые заложил в неё программист. Они имеют возможность учиться на предшествующих событиях – как на аномальном, так и на нормальном трафике. За счёт этого достигается высокая эффективность и адаптивность СОА.

Сетевой трафик в реальном времени обрабатывается при помощи многослойного персептрона, обученного распознавать атаки на основе анализа параметров заголовков и порций данных. Сообщения о зарегистрированных атаках накапливаются в буфере сообщений (рис.3). Через заданные промежутки времени сообщения передаются для анализа блоку корреляции, который формирует кластеры сообщений, относящихся к конкретным планам атак. После этого сообщения из буфера сохраняются в архивной базе данных для проведения корреляционного анализа за более значительный промежуток времени, и далее буфер очищается.

Результаты работы модуля корреляции попадают на входы нейросети типа многослойный персептрон, обученный распознавать последовательности наборов признаков (сообщений), характеризующих определённый план атаки. По результатам распознавания можно определить, на какой стадии осуществления находится обнаруженная атака, и предсказать её развитие.

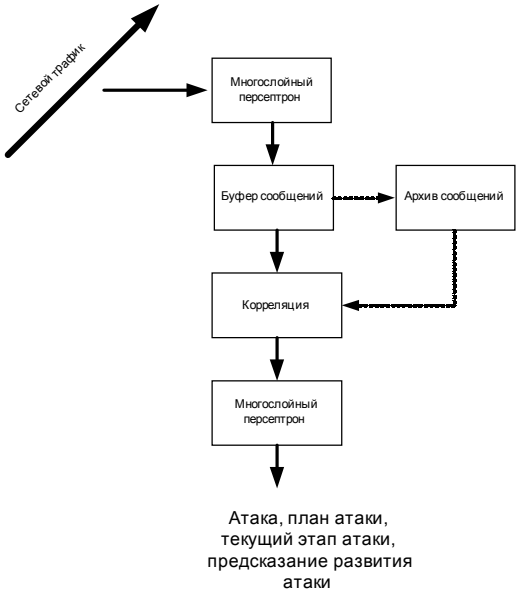

Рис.1. Архитектура СОА

Пусть для реализации атаки необходимо предпринять ряд последовательных шагов: сбор разведывательной информации, проникновение, получение привилегий, выполнение определённых действий и т.п. Тогда этапы реализации можно организовать в «план атаки». Назначение модуля корреляции – на основании сообщений об атаках распознать план атаки.

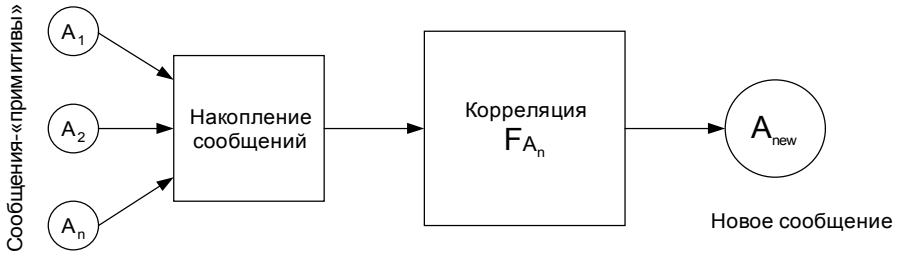

Рис.2 . Подсистема корреляции сообщений об атаках

Корреляция позволяет решить следующие проблемы:

– уменьшить число ложных срабатываний (false positive);

– уменьшить число пропуска атак (false negative);

– получить более полную и точную информацию о причине возникновения предупреждения.

Таким образом, предлагаемый комбинированный метод обнаружения аномалий основан на использовании нейронной сети, исключающий возможность враждебного переобучения. Этот метод отличается возможностью обнаруживать известные и выявлять новые аномалии трафика.

Для моделирования сетевых атак и анализа защищённости удалённой сети или конкретного хоста разработан макет (рис.3) и программа имитации сетевых атак, позволяющая тестировать саму систему обнаружения атак [2].

Назначение системы:

- анализ защищённости сети (зондирование);
- тестирование систем обнаружения атак;
- изучение механизмов реализации сетевых атак.

Возможность имитации следующих типов атак:

- отказ в обслуживании;
- распределённый отказ в обслуживании;
- скрытое сканирование;
- составление карты атакуемой сети;
- атаки на сетевые сервисы: ftp, telnet, dns, rpc, netbios, web-cgi, web-iis и др.

Такого рода система дает возможность обработки ответной реакции атакуемого хоста и генерации трафика с характеристиками, задаваемыми пользователем в реальном времени.

Ведется разработка инструментального средства для автоматизированного обнаружения уязвимостей. В настоящее время не существует стандартизированных средств, осуществляющих атакующие действия, которые можно было рекомендовать для проведения испытаний. В то же время особенности программы имитации атак позволяют использовать её для создания реалистичных интерактивных тестов.

Рассмотренные выше научно-технические разработки по системам обнаружения вторжений переданы Заказчикам и успешно используются в учебном процессе по курсам «Методы и средства защиты компьютерной информации» и «Защита информации в компьютерных системах». В 2005 г. под руководством профессора Макаревича О.Б. была успешно защищена кандидатская диссертация Абрамовым Е.С. на тему разработки методов и средств создания построения систем обнаружения атак.

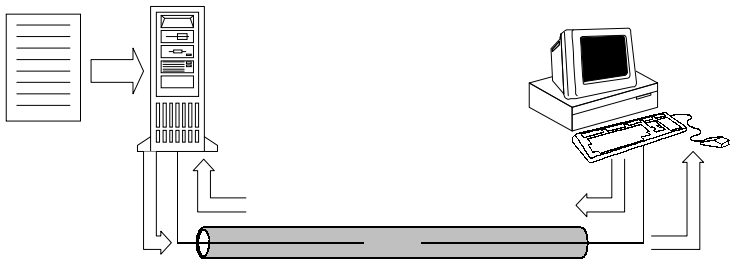

Рис.3. Структура макета имитации сетевых атак

Проблема использования биометрических технологий в управлении доступом является одной из наиболее динамично развивающихся областей информационной безопасности. Аналитики отмечают, что рынок биометрических технологий становится все в большей мере коммерчески выгодным (рис.4).

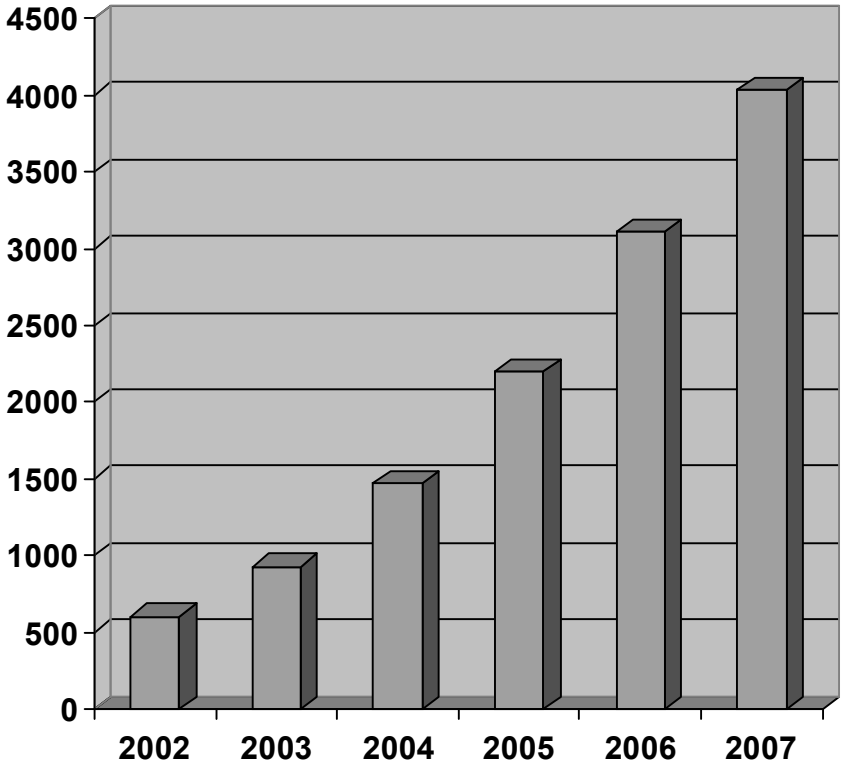

Рис. 4. Объем рынка биометрических технологий по данным International Biometric Group на период с2002 по 2007 гг. (в млн.долл.)

В настоящее время проводятся интенсивные исследования, направленные на расширение возможностей биометрии в таких методах идентификации (рис.5), как:

- по отпечаткам пальцев, ладони;
- по геометрии руки;
- по отпечаткам ладони;
- по строению кровеносных сосудов;
- по томографии лица;
- по форме лица в 2-х и 3-х мерном измерении;
- по голосу;
- по запаху;
- по подписи;
- по динамике печатания;
- по радужной оболочке или сетчатке глаза;

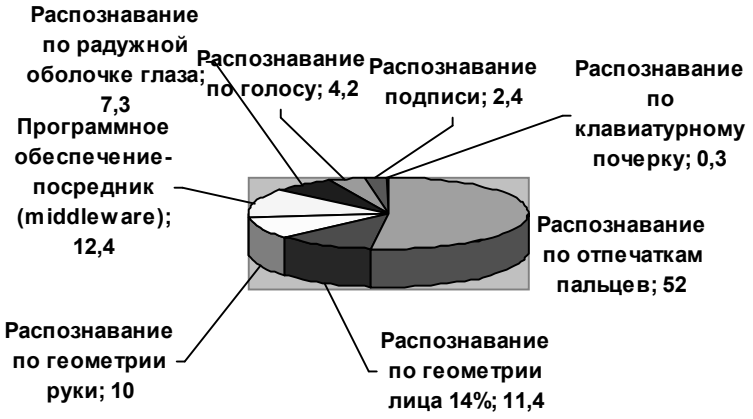

Рис.5. Сегментация рынка согласно данным International Biometric Group

Разработки в данной области, проводимые на кафедре БИТ ТТИ ЮФУ, касаются голосовой аутентификации пользователей персональных компьютеров, систем скрытого клавиатурного мониторинга пользователей автоматизированных информационных систем и, наконец, систем биометрической криптографии [3-6].

Системы аутентификации по голосу применимы там, где использование других методов практически невозможно, например, для предоставления удаленного доступа к услугам и данным по телефонным каналам или через Internet. Широкое применение биометрических систем влечет за собой повышенный интерес со стороны злоумышленников, направленный на разработку атак по их взлому. Наиболее часто применяемой является replay-атака, суть которой заключается в том, что в систему передаются биометрические признаки, предъявленные ранее, например, силиконовый муляж пальца или магнитофонная запись парольной фразы. Таким образом, разработку систем такого рода необходимо вести с учетом защиты их от этих атак. Одной из перспективных, с точки зрения защиты от replay-атак, может быть система аутентификации, основанная на предъявлении случайно сформированной последовательности ключевых слов из словаря фиксированного размера. Тогда задачи, решаемые такой системой, можно разделить на две части. Первая – собственно решение задачи голосовой аутентификации, при этом разрабатываемый метод должен быть контекстно-независимым. Вторая заключается в решении задачи распознавания изолированных слов независимо от голоса диктора. При этом в системе предусматривается возможность смены всех ключевых слов. На тему разработки методов и средств голосовой аутентификации, затрудняющих проведение replay-атак, на кафедре БИТ ТТИ ЮФУ под руководством профессора Бабенко Л.К. в 2006 г. успешно защищена кандидатская диссертация Юрковым П.Ю. [3,4], в которой решены следующие задачи.

1. Разработана новая математическая модель системы речевосприятия на основе методов вэйвлет-анализа, отличающаяся простотой реализации и возможностью быстрой адаптации под решаемую задачу за счет изменения шага масштабирования. Благодаря объединению вэйвлет-функций с функцией компенсации громкости на разных частотах впервые появилась возможность получения модели первичной обработки сигнала в системе речевосприятия в виде единого преобразования. Разработанный на основе данной модели метод формирования векторов речевых признаков за счет использования нейронных сетей (НС) с узким горлом позволяет получать компактные векторы признаков, которые в сжатом виде со-

держат информацию как о частотных, так и о временных характеристиках речевого сигнала, что намного информативнее стандартных методов, содержащих только частотные характеристики.

2. Разработан нейронечеткий метод распознавания фонем, который позволяет за счет использования НС выполнять процедуру фаззификации над многомерными векторами речевых признаков. Использование дихотомических признаков акустической классификации звуков позволяет более точно распознавать речевой сигнал, а также анализировать полученные результаты в виде терминов естественного языка за счет применения алгоритмов нечеткого вывода.

3. Разработаны алгоритм распознавания, эталонная модель и методы формирования шаблона слова, которые позволяют выполнять распознавание без этапа обучения за счет использования нечетких функций и методов нечеткого динамического программирования. Разработанные средства позволяют создавать подсистемы контроля ключевых слов с возможностью быстрой смены всего множества слов. Благодаря этому система аутентификации диктора, основанная на данной подсистеме, удовлетворяет выработанным требованиям безопасности и способна затруднить или предотвратить возможность проведения replay-атаки.

4. Проведены экспериментальные исследования с целью выбора параметров распознавания для эффективного решения задачи аутентификации диктора. В результате удалось получить стабильные биометрические признаки, определить характеристики НС, обладающей лучшими обобщающими способностями, и достичь уровня EER ошибки, равного 1.3%, что лучше аналогичных текстонезависимых систем аутентификации.

5. Разработан лабораторный практикум по изучению методов и систем биометрической аутентификации [5]. Работа посвящена вопросам практического изучения функционирования, а также методов оценки характеристик биометрических систем.

Для решения задач регистрации и аутентификации пользователя. использованы искусственные нейронные сети. Работа студентов с программным комплексом состоит из следующих основных этапов.

1. Запись голоса регистрируемого пользователя.

2. Создание биометрического шаблона пользователя. Заключается в удалении пауз шумных участков речи, выделении биометрических параметров обучения искусственной нейронной сети с архитектурой многослойный персептрон.

3. Аутентификация пользователя на основе созданного ранее шаблона.

Успешная аутентификация представляется значением выхода нейронной сети для аутентифицируемого диктора. Распределения вероятностей P_p ответов нейронной сети на голос зарегистрированного и незарегистрированного пользователей рассчитываются на основе десятикратных попыток аутентификации. Соотношения этих распределений определяют ошибки первого (отказ своему) и второго (пропуск чужого) рода. Студенты при выполнении работы практически реализуют все три этапа биометрической голосовой аутентификации, используя в качестве дикторов себя и своих согруппников, строят графики распределений вероятностей, определяют ошибки первого и второго рода.

Разработка методов скрытого клавиатурного мониторинга ведется на кафедре БИТ в течение ряда лет, при этом получены достаточно серьезные результаты [6]. Большая часть из них представлена в кандидатской диссертации Казарина М.Н.. В ней предложена организация системы скрытого клавиатурного мониторинга на основе выделения информативных параметров, многосвязного представления и последовательной классификации особенностей динамики работы на клавиатуре. Предложенный метод классификации основывается на анализе устойчи-

вых последовательностей событий клавиатуры, которые образуются во время работы пользователя на компьютере.

При решении поставленных в работе задач получены следующие научные результаты.

1. Разработаны методы выделения наиболее информативных параметров особенностей динамики работы на клавиатуре, которые заключаются в использовании последовательно-временных фильтров. Предлагаемые методы позволяют не только выявить параметры, характеризующие динамику работы на клавиатуре, но и уменьшить ошибки первого и второго рода, что немаловажно для биометрических систем контроля доступа.

2. Впервые разработан метод многосвязного представления особенностей динамики работы на клавиатуре, основанный на устойчивых последовательностях событий клавиатуры. Предложенный метод основывается на предположении, что большей информативностью обладают не значения времен удержаний и пауз между удержаниями клавиш (такой подход используется в существующих методах), а устойчивые последовательности сочетаний значений этих времен.

3. Разработан последовательный метод классификации на основе многосвязного представления особенностей динамики работы на клавиатуре, который использует в качестве числовой характеристики вес устойчивой последовательности и позволяет реализовать непрерывную процедуру аутентификации. Предложен способ оценки веса устойчивых последовательностей, основанный на вероятностных характеристиках последовательностей событий клавиатуры.

4. Разработана программная модель клавиатурного мониторинга на основе многослойного представления особенностей динамики работы на клавиатуре с помощью быстрого алгоритма кластеризации и последовательного метода классификации устойчивых последовательностей событий клавиатуры, с применением последовательно-временных фильтров (временного и клавиатурного) для выделения наиболее информативных параметров.

5. Получены экспериментальные оценки разработанных методов скрытного клавиатурного мониторинга с помощью созданной программной модели и сравнение с существующими аналогами. На основе полученных экспериментальных оценок сделаны выводы о работоспособности предложенных методов скрытного клавиатурного мониторинга и применимости их в реальных системах анализа особенностей динамики работы на клавиатуре. В ходе экспериментов были получены результаты, свидетельствующие о малой информативности событий удержания клавиш. Использование событий удержания клавиш при анализе особенностей динамики работы на клавиатуре привело к увеличению ошибок первого и второго рода.

Все результаты исследований реализованы в виде лабораторных работ по курсу «Методы и средства защиты компьютерной информации».

С 2002 г. на кафедре БИТ ТТИ ЮФУ ведутся исследования в области разработки биометрических криптосистем. В частности, в работах [7-10] предложен метод генерации криптографических ключей по голосовому паролю. Разработанный метод состоит из двух этапов: сохранение криптографического ключа пользователя и восстановления криптографического ключа (рис.6). В соответствии с предложенным методом была реализована программная система преобразования голосового пароля в криптографический ключ. В экспериментах по тестированию данной системы участвовало 20 дикторов различных возрастов без явных отклонений в произношении. В качестве *PPK* используется случайно сгенерированный криптографический ключ размерностью 32 бита. В качестве *RBS* используются случайным образом сгенерированные битовые наборы размерностью 32 бита. По-

лученная обучающая выборка используется для обучения трехслойного персептрона.

Для обучения сети использована одна из модификаций метода обратного распространения ошибки – resilent backpropagation. В процессе экспериментов контролировались такие параметры, как вероятность неправильного восстановления ключа при правильных голосовых данных (false rejection rate, FRR), вероятность правильного восстановления ключа при неверных голосовых параметрах (false acceptance rate, FAR), время обучения и время тестирования в секундах. Общее число экспериментов составило более 10^6.

Подробно результаты экспериментов приведены в работе [8] и частично в [9,10]. Коротко результаты можно охарактеризовать следующим образом. Среднее значение FAR=0,00125, среднее значение FRR порядка 0,20, вероятность двукратного ложного отказа FRR около 0,1, а трехкратного - менее 0,04. Объем памяти для хранения параметров нейронных сетей менее 40 Кб для одного пользователя. Время восстановления ключа около 2 с.

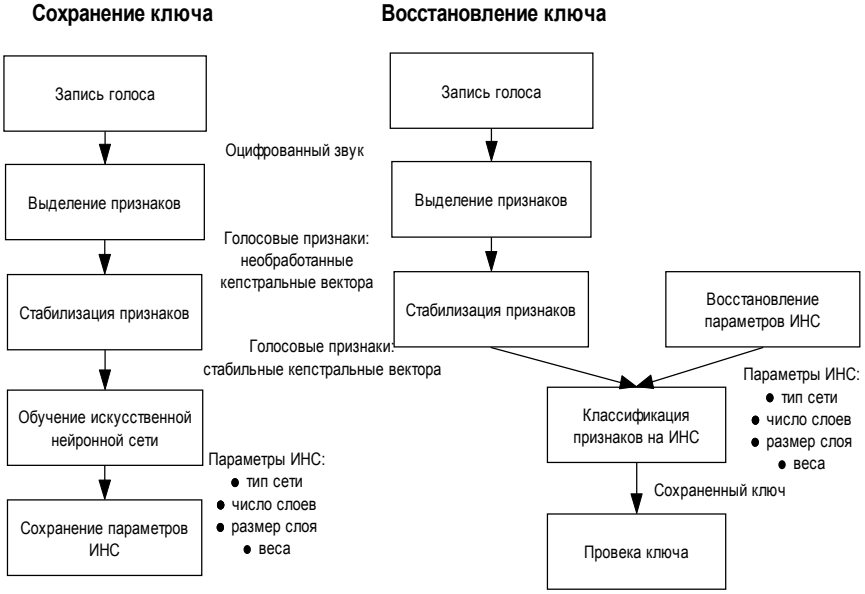

Рис. 6. Метод генерации ключей по голосовому паролю

Другое перспективное направление применения метода – безопасное хранение криптографических ключей на мобильных устройствах, таких как смартфоны, коммуникаторы и микрокомпьютеры.

Кроме того, биометрическая аутентификация и биокриптография находят применение в качестве методов управления доступом для мобильных телефонов. В перспективе разработка методов клавиатурной биокриптографии.

Биометрическая криптография позволяет решить основные проблемы безопасности, возникающие при практической эксплуатации систем биометрической идентификации. При реализации последнего направления также широко применяются искусственные нейронные сети.

Проблема управления доступом в СУБД. Использование СУБД, как надежной основы для построения ИС, связано с проблемой разграничения доступа пользователей к хранимой информации.

Согласно анализу причин нарушений безопасности 89% недостатков средств защиты в ИС приходится именно на долю системы разграничения доступа.

Среди существующих моделей разграничения доступа (дискреционная, ролевая, мандатная и другие) особого внимания требует модель мандатного доступа.

Её особенность состоит в предотвращении возможности преднамеренного или случайного понижения ценности информации за счёт её утечки (умышленного переноса).

Кроме того, с помощью мандатной модели возможно существенное упрощение задачи администрирования ИС во время установки и эксплуатации, что приводит к уменьшению количества ошибок.

В настоящее время вопрос разработки механизмов и средств обеспечения мандатного доступа в ИС и в СУБД, в частности, недостаточно проработан, так как является задачей нетривиальной и трудоемкой и требует детальной проработки правил общей мандатной модели Белла-Ла-Пападула.

Небольшое количество существующих промышленных СУБД (в частности, Oracle и Линтер) имеют собственную систему мандатного разграничения доступа. Однако, анализ этих систем показал, что реализуемые ими модели не обладают полнотой и корректностью реализации.

В настоящее время на кафедре БИТ проводятся работы по созданию эффективного метода доступа в СУБД с использованием мандатного разграничения. При этом разрабатывается оригинальная модель, формализующая правила доступа к базам данных, таблицам и записям, а также методы обеспечения защищенного хранения, надежной идентификации и аутентификации прав мандатного доступа. Предложена и реализуется интересная идея использования здесь цифровых сертификатов (рис.7) [11].

Отдельные вопросы по защите баз данных рассматриваются совместно с лабораторией ФПИБ КБНЦ РАН.

В частности выполняется совместный проект РФФИ № 06-07-96608-р_юг_а «Разработка и внедрение новых технологий комплексной защиты многопользовательских региональных ГИС».

Для студентов специальностей направления «Информационная безопасность» реализован комплекс программ и создан лабораторный практикум по изучению иерархии систем удостоверяющих центров [12].

Проблема анализа стойкости систем защиты информации существует при разработке и совершенствовании алгоритмов защиты дискретной информации и напрямую связана с необходимостью проведения объемных многовариантных вычислений.

Эффективность некоторых методов оценки стойкости можно увеличить при помощи распределенных вычислений, средства реализации которых постоянно совершенствуются.

Это позволяет сократить временные затраты и получать более адекватные оценки при реализации существующих методов [13,17].

Работы в области анализа стойкости защиты информации проводятся в двух направлениях.

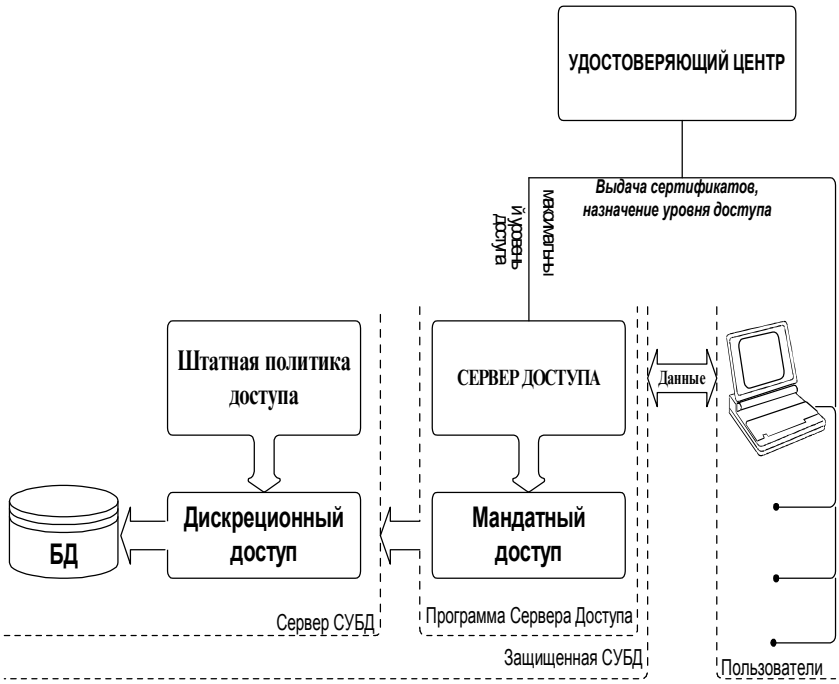

Рис.7. Схема разграничения доступа

1. *Изучение современных методов криптоанализа.* С одной стороны, эта тематика, в современном мире имеет полузакрытый характер. Публикации в открытой печати весьма скудны. С другой стороны – явная необходимость понимания свойств соответствующих преобразующих функций с целью улучшения эффективности их реализации. В этом плане нами рассмотрен ряд существующих методов, таких как линейный и дифференциальный криптоанализ, их комбинация, метод слайдовой атаки, атака «квадрат», метод «согласований», связанный с решением задачи разложения на множители, дискретного логарифмирования в конечном поле Галуа и в точках эллиптической кривой, метод Полларда для дискретного логарифмирования в точках эллиптической кривой. Для рассмотренных методов составлены подробные методики применения их для анализа блочных шифров DES, двукратного DES, AES, ГОСТ 28147 – 89, RC 5, общей схемы сети SPN (Substitution – Permutation Network). Проведено численное моделирование большинства методов, выявлены некоторые ограничения их применимости по числу раундов шифрования, длине ключа, другим параметрам. Для использования в учебном процессе полученных результатов составлены соответствующие практикумы и лабораторные работы, базирующиеся на применении указанных выше современных методов криптоанализа к понятным, специально разработанным «учебным» криптографическим алгоритмам, сохраняющим основные свойства действующих алгоритмов, но имеющих упрощенную конфигурацию по числу раундов шифрования, размеру шифруемых блоков и длине криптографического ключа.

В настоящее время используется 5 лабораторных работ/14-16/.

1. Изучение метода линейного криптоанализа применительно к алгоритмам шифрования, построенным по схеме Фейстеля.

2. Изучение метода дифференциального криптоанализа применительно к алгоритмам шифрования, построенным по схеме Фейстеля.

3. Изучение метода дифференциального криптоанализа применительно к многораундовым алгоритмам шифрования, построенным на основе сети SPN.

4. Изучение метода линейного криптоанализа применительно к многораундовым алгоритмам шифрования, построенным на основе сети SPN.

5. Изучение метода слайдовой атаки на примере алгоритмов шифрования, построенных по схеме Фейстеля.

Разработанные лабораторные работы используются для курсов «Программно-аппаратная защита информации», «Криптографическая защита информации», «Криптографические методы и средства обеспечения информационной безопасности» при обучении студентов специальностей 090103, 090104.

2. Распараллеливание алгоритмов криптоанализа, реализация с помощью современных средств программирования, оценка эффективности.

При рассмотрении вопросов распараллеливания задач криптоанализа получены следующие результаты [17,18].

1. Разработаны параллельные алгоритмы "распределенных согласований", позволяющие на n-мерной вычислительной системе решать важные задачи, сводящиеся к решению уравнения вида $\psi(k') = \gamma(k'')$, где $\psi(k'), \gamma(k'')$ – нелинейные функции, $k' \in F_{n_1}$, $k'' \in F_{n_2}$, $(k', k'') = k$, $k \in F_n$, $F_{n_1} \times F_{n_2} = F_n$.

2. Параллельные алгоритмы "распределенных согласований" для анализа каскадных шифров. Полученные оценки эффективности распараллеливания алгоритмов (ускорение $R = T_1 / T_w$, где T_1 – время решения задачи на однопроцессорной системе, а T_w – время решения той же задачи на w – процессорной системе) "распределённых согласований" для анализа безопасности двойного *DES* показывают, что $R = \dfrac{w}{1 + 0{,}115 \cdot w}$, где w – количество процессоров.

3. Параллельные алгоритмы "распределенных согласований" для отыскания дискретного логарифма в конечных полях и в группе точек эллиптической кривой над конечным полем. Полученные теоретические оценки эффективности распараллеливания алгоритмов "распределённых согласований" для решения задачи дискретного логарифмирования в конечном поле показывают, что R, например, при $w = 2$ и $t = 1700$ будет составлять 1,83.

Инструментальной основой распределенных вычислений могут служить современные пакеты прикладных программ для кластерных систем. В качестве такого пакета нами выбран «Интерфейс передачи сообщений» (Message Passing Interface, или, сокращенно MPI) за свою многоплатформенность, удобный интерфейс, гибкую конфигурацию и легкую переносимость с одной вычислительной машины на другую. При использовании пакета MPI считается, что компьютер состоит из нескольких процессоров, каждый из которых снабжен своей собственной памятью. Параллельная программа в модели передачи сообщений представляет собой набор обычных последовательных программ, которые обрабатываются одновременно. Обычно каждая из этих последовательных программ выполняется на своем процессоре и имеет доступ к своей, локальной памяти. Пакет MPI служит для обеспечения согласованной работы параллельных частей программы. Явным достоинством при такой организации вычислений является возможность написания и отладки программы на однопроцессорной системе. При разработке программ для тестирования алгоритмов шифрования с помощью многопроцессорных вычислительных систем, необходимо учитывать такие особенности, как число раундов, используемых в тестируемом алгоритме и количество данных, требуемое для успешного проведения атаки. Как правило, криптоаналитические атаки проходят в два этапа. На первом этапе выполняется первичная обработка параметров алго-

ритма и подготовка всех данных для проведения анализа, которые, как правило, осуществляет один процессор, называемый главным. Второй этап состоит в непосредственном анализе алгоритма, что в большинстве случаев сводится к нахождению секретного ключа, использованного для шифрования данных с помощью исследуемого алгоритма. При этом должна быть организована правильная и грамотная взаимосвязь частей программы, выполняющих вышеуказанные этапы. Кроме того, программа должна позволять использовать в вычислениях любое число процессоров, при этом с помощью разработанного алгоритма данные для анализа должны распределяться равномерно.

В настоящее время проводятся исследования по распараллеливанию дифференциального криптоанализа на всех этапах его выполнения.

Совместно с лабораторией ФПИБ КБНЦ РАН проводятся работы по определению возможностей распараллеливания следующих методов дискретного логарифмирования: Гельфонда, «giant step-baby step», встречи на случайном дереве, базы разложения, решета числового поля, диофантовой аппроксимации, Полларда, непрерывных дробей, квадратичного решета.

Благодаря оперативному использованию результатов НИОКР в учебном процессе студенты, магистранты, аспиранты и преподаватели могут легко осваивать современные средства защиты информации и повышать свою квалификацию.

Работа выполнена при поддержке грантов РФФИ № 06-07-89010 и № 07-07- 00138

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Абрамов Е.С., Бабенко Л.К., Макаревич О.Б., Пескова О.Ю.* Разработка архитектуры СОА на основе нейронной сети Изд-во ТРТУ. Материалы VI Международной научно-практической конференции «Информационная безопасность». – Таганрог, 2004.

2. *Абрамов Е.С., Макаревич О.Б.* Программный имитатор сетевых атак . Международная научно-практическая конференция и Российская научная школа молодых ученых и специалистов «Системные проблемы качества, математического моделирования информационных и электронных технологий» 1-12 октября 2003 Сочи.

3. *Юрков П.Ю.* Автореферат на соискание степени кандидата технических наук «Разработка и исследование методов и средств голосовой аутентификации с динамически изменяемым множеством ключевых слов». – Таганрог. 2006.

4. *Макаревич О.Б., Бабенко Л.К., Федоров В.М., Юрков П.Ю.* Текстонезависимая аутентификация / идентификация по голосу в системах управления доступом.– X Всероссийская научно-практическая конференция “Проблемы информационной безопасности в системе высшей школы”.– М: МИФИ, 2003.- С. 28-29.

5. *Бабенко Л.К., Тумоян Е.П., Юрков П.Ю.* Лабораторный практикум по изучению методов и систем биометрической аутентификации. – Таганрог, ТРТУ, 2004. –14 с.

6. *Брюхомицкий Ю.А., Казарин М.Н.* Скрытый клавиатурный мониторинг операторов автматизированных информационно-управляющих систем. Сб. тезисов и докладов V11 Всероссийская научная конференция студентов и аспирантов «Техническая кибернетика, радиоэлектроника и системы управления», 2004 г., С. 357-358.

7. *Бабенко Л.К., Макаревич О.Б., Тумоян Е.П.* Перспективы развития биокриптографии. Известия - ТРТУ. Материалы V11 Международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во. ТРТУ, 2005. №4 (48), – 250 с.

8. *Макаревич О.Б., Тумоян Е.П.* // Известия ТРТУ. Таганрог: 2003. № 4. С.132-141.8.

9. *Makarevich O. B., Babenko L.K., Tumoyan E.P.* // Proc. IEEE AIS’04 and CAD -2004. 2004. P. 61- 66.

10. *Makarevich O. B., Babenko L.K., Tumoyan E.P.* // Proc. Intern. Scientific Workshop “High-performance computing systems”. 2004. P. 214 - 218.

11. *Бабенко Л.К., Басан А.С., Макаревич О.Б.* Организация мандатного доступа к данным ГИС на основе сертификатов // Сб. тр. Международной научно-технической конференции, посвященной 225-летию МИИГАиК М. 2004

12. Лабораторный практикум по изучению системы удостоверяющих центров и сертификатов открытых ключей №3619. – Таганрог: Изд-во ТРТУ, 2004. – 31с.

13. *Бабенко Л.К., Ищукова Е.А.* «Современные алгоритмы блочного шифрования и методы их анализа», – М.: Гелиос, 2006. – 375с.

14. *Бабенко Л.К., Ищукова Е.А.* Изучение метода линейного криптоанализа применительно к алгоритмам шифрования, построенным по схеме Фейстеля.. – Таганрог, Изд-во ТРТУ, 2004. – 21 с.

15. *Бабенко Л.К., Ищукова Е.А*. Изучение метода дифференциального криптоанализа применительно к алгоритмам шифрования, построенным по схеме Фейстеля. – Таганрог, Изд-во ТРТУ, 2004. – 15 с.

16. *Бабенко Л.К., Ищукова Е.А*. Изучение метода слайдовой атаки на примере алгоритмов шифрования, построенных по схеме Фейстеля. – Таганрог, Изд-во ТРТУ, 2004. 24 с.

17. *Бабенко Л.К.,. Курилкина А.М*. Параллельный алгоритм «распределенных согласований» решения задачи дискретного логарифмирования в конечных полях. Журнал «Вопросы защиты информации». – М: «ФГУП «ВИМИ», 2005, №2 (69), – С.8-14.

18..*Курилкина. А.М.* Автореферат кандидатской диссертации «Оценка вычислительной стойкости защиты информации алгоритмами «распределенных согласований». – Таганрог, Изд-во ТРТУ, 2005. – 16 с.

А.И. Грюнталь
Россия, г. Москва,
Научно-исследовательский институт системных исследований РАН

ИНФОРМАЦИОННО – БЕЗОПАСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

1. Постановка задачи

В 1995 г. в НИИСИ РАН была поставлена задача создания отечественного комплекта средств общего программного обеспечения (ОПО) для вычислительных систем, функционирующих в реальном масштабе времени, удовлетворяющих требованиям информационной безопасности (ИБ) и технологической независимости (ТН). Информационная безопасность – это отсутствие в исполняемом коде программ недекларированных функций и/или закладных элементов. Технологическая независимость – это гарантированная возможность сопровождения программы на всех этапах жизненного цикла коллективами, работающими в РФ, без прямого или косвенного участия зарубежных специалистов. Разрабатываемый комплект средств ОПО также должен был быть лицензионно – чистым. Основное внимание уделялось разработке операционной системе реального времени, с учетом требований гарантированного быстродействия, и компилятора – основного технологического средства разработки прикладного ПО.

2. Информационная безопасность и технологическая независимость

Группы требований по ИБ и ТН формально различны. Соответствие требованиям ИБ подтверждается процедурами сертификации, основанной на анализе исходного текста программного средства. Обеспечение адекватности исходного и загрузочного текста программ требует применения сертифицированных инструментальных средств, в частности средств кодогенерации.

Эффективность формальных процедур выявления недекларированных возможностей и/или закладных элементов путем анализа исходного текста ограничена большим объемом и большой сложностью программ. Например, исходный текст Си-компилятора включает порядка 2-х миллионов строк. Содержательный и полный анализ программы такого объема требует квалификации разработчика этой программы. Неизбежно имеющиеся ошибки в программах такой сложности могут интерпретироваться при сертификации как закладные элементы. Поэтому