УДК 004.037

О.Б.Макаревич

ОСНОВНЫЕ НАПРАВЛЕНИЯ НАУЧНЫХ РАЗРАБОТОК КАФЕДРЫ БИТ ТТИ ЮФУ И ИХ ВНЕДРЕНИЕ В НИОКР И УЧЕБНЫЙ ПРОЦЕСС

Кафедра безопасности информационных технологий (БИТ) была организована в 1996 году. Сейчас коллектив кафедры имеет в своем составе 23 единицы ППС и 10 единиц УВП (рис. 1).

Рис. 1. Структура кафедры безопасности информационных технологий

Работы по информационной безопасности на кафедре ведутся по направлениям:

- подготовка, повышение квалификации и переподготовка кадров;
- проведение исследований и разработок, направленных на внедрение в сфере науки и производства безопасных информационных технологий.

Основная тематика научно-исследовательских и отытно-конструкторских работ, проводимых в интересах государственных структур и частных фирм; реализуется в рамках научной школы «Интеллектуальные системы защиты информации на базе нейросетевых технологий». Конкретно при этом решаются следующие проблемы:

- защиты компьютерной сети от несанкционированных вторжений;
- использования биометрических технологий в управлении доступом;
- анализа стойкости систем защиты информации;
- стеганографии и стегоанализа;
- защиты баз данных (защита ГИС).

Результаты НИОКР широко используются в учебном процессе, что позволяет повысить качество подготовки специалистов.

Защита компьютерной сети от несанкционированных вторжений является в настоящее время основной проблемой для всех государственных организаций и частных фирм. Особенно остро стоит этот вопрос для критических производств (атомная энергетика, железнодорожный транспорт, авиация, химическое производство и т.д.). 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 необходимость разработки более эффективных инструментов противодействия нарушителям. К таким инструментам относятся системы обнаружения атак (СОА), представляющие собой программно-аппаратные комплексы, предназначенные для выявления несанкционированных действий в ИС. 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. 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.

По тематике обнаружения вторжений на кафедре успешно защищены три кандидатские диссертации, ведутся научно-исследовательские работы с Заказчиками.

Использования биометрических технологий в управлении доступом является одной из наиболее динамично развивающихся областей информационной безопасности. Разработки в данной области, проводимые на кафедре, касаются голосовой аутентификации пользователей компьютеров, систем скрытого клавиатурного мониторинга пользователей АС и систем биометрической криптографии. Все данные работы ведутся на кафедре в виде соответствующих НИР.

Анализу стойкости систем защиты информации посвящены две монографии профессора Бабенко Л.К. вместе с соавторами. Результаты исследований широко используются для постановки лабораторных и практических работ по курсу «Аппаратно-программные средства защиты».

По направлению стеганографии и стегоанализ на кафедре были разработаны методы и алгоритмы анализа аудиосигналов и изображений, содержащих скрываемую информацию стеганографическими методами на основе замены наименее значащих бит. Разработан метод разностного стегоанализа изображений. Для стегоанализа мультимедийных сообщений разработаны универсальные методы, основанные на декомпозиции анализируемых данных при помощи вейвлет-преобразования с последующей оценкой субполос разложения. Дальнейшим раз-

витием данного метода является распознавание файлов, содержащих скрытые данные нейросетевыми технологиями с использованием признаков, полученных на основе вейвлет-декомпозиции. Необходимо отметить, что в настоящее время методы компьютерной стеганографии используются не только для целей защиты информации, но и для целей охраны интеллектуальной собственности. Основным направлением развития стеганографических методов является скрытие данных непосредственно в потоке информации, обладающей избыточностью. Необходимо отметить, что популярность и доступность стеганографического программного обеспечения привела к тому, что методы компьютерной стеганографии используются для скрытой передачи информации преступными элементами, в том числе членами преступных группировок, террористами и т.д. В этих условиях важное значение приобретает развитие существующих и разработка новых методов и средств стегоанализа – методов и средств обнаружения несанкционированной передачи сообщений, скрытых путем стеганографического преобразования.

Тематика по защите баз данных (защита ГИС) востребована достаточно широко. На сегодняшний день наибольшее распространение получили реляционные системы управления базами данных (СУБД) и геоинформационные системы. Кафедрой БИТ ТРТУ разработаны алгоритмы, механизмы и программные средства обеспечения мандатного доступа в уже существующих и действующих СУБД и ГИС. Причем внедрение такой защиты не требует изменения самой информационной системы.

Предлагаемый механизм обеспечения мандатного доступа состоит в том, что всем пользователям выдаются цифровые сертификаты открытых ключей, являющиеся мандатами на возможность работы с данными различной степени конфиденциальности. Пользователь имеет право работать с информацией только той категории конфиденциальности, которая разрешена ему сертификатом. Структура сертификата, а также метод аутентификации с использованием отрытых ключей и ЭЦП описаны в известных требованиях X.509 v.3.

Сертификаты генерируются и выдаются пользователям системой удостоверяющих центров. Все сертификаты защищены ЭЦП удостоверяющего центра, выдавшего его, – это исключает подделку. Удостоверяющий центр выполняет административные функции, выдавая пользователям сертификаты и тем самым разрешая законному владельцу сертификата работать с данными ИС.

Механизм обеспечения мандатного доступа основывается на введении специального диспетчера доступа, который анализирует и модифицирует определенным образом запросы пользователей к базе данных. Таким образом, для пользователей штатная политика доступа подменяется политикой диспетчера доступа. А задача мандатного доступа сводится к тому, что ИС посредствам Диспетчера Доступа предоставляет пользователю только ту информацию, которая соответствует уровню доступа из сертификата.

Проблема распознавания изображений текстовых документов.

Вследствие постоянного роста мощности ЭВМ и объемов обрабатываемой информации все более актуальной становится проблема ввода данных. Об этом свидетельствует появление все новых средств ввода и не прекращающиеся исследования в этой области. В качестве примеров результатов таких исследований можно привести появление большого количества самых разнообразных систем распознавания речи и систем распознавания изображений текстовых документов (OCR-систем, от английского Optical Character Recognition).

Однако большинство OCR-систем требуют высокого качества твердой копии документа и высокого разрешения при сканировании. Но на практике часто возни-

кает необходимость ввода в ЭВМ большого объема текстовой информации, представленной в виде изображений документов низкого разрешения и качества, но при этом вполне приемлемого для визуального прочтения.

Были предложены методы, на основе которых было реализовано на практике распознавание английских текстов, напечатанных с использованием шрифтов из ограниченного набора. Твердая копия была получена с помощью струйного принтера. Для чистоты эксперимента был выбран полуторный интервал между строками и разреженный на 1 пункт межсимвольный интервал. Был получен готовый текст, ошибок в нахождении строк и слов практически не было, качество распознавания букв 94-100% в зависимости от экземпляра изображения.

Проблемы идентификации цифровой аппаратуры записи по создаваемым записям на примере идентификации цифровых фотокамер и цифровых микрофонов.

За последние десятилетия вместе с массовым вытеснением аналоговых средств звуко- и видеозаписывающей техники компактными цифровыми устройствами стала актуальной задача их идентификации, а также подтверждения подлинности получаемых с их помощью образов. Известными аналогами являются идентификация печатающего устройства по оттиску литер, диктофона по набору гармоник тракта записи и воздействию лентопротяжного механизма на плёнку, фотокамер по форме границ окна кадра и следам, оставляемым механизмом перемотки плёнки. Как известно, аналоговые и цифровые образы, полученные при помощи любого устройства записи, несут в себе набор особенностей, сформированных различными узлами тракта записи, что позволяет (при наличии предполагаемого устройства записи) во многих случаях однозначно установить принадлежность ему образа. Помимо идентификации, уникальные признаки устройства могут быть использованы для обнаружения следов монтажа.

Ввиду того, что в тракт записи устройства входят как аналоговый, так и цифровой участки, можно выделить следующие классы признаков:

1. Признаки аппаратной части, а именно отклонения в пределах допусков характеристик чувствительного элемента и аналоговых блоков обработки до АЦП. В общем случае признаки данного класса позволяют идентифицировать конкретный экземпляр устройства. В качестве примеров можно привести отклонения в пределах допусков светочувствительных элементов матриц фото и видеокамер, отклонения от средней АЧХ-микрофона, внутренние наводки на аналоговую часть цифровых диктофонов и микрофонов, отклонения характеристик АЦП и т.д.

2. Признаки программной части, а именно алгоритмов постобработки сигнала. Примерами алгоритмов для цифровых камер являются алгоритмы подавления дефектов матрицы, восстановления изображения из структуры Байера, повышения субъективного качества изображения. Для цифровых микрофонов примерами являются алгоритмы выравнивания АЧХ, подавления эхо-эффекта, шумоподавления. Идентификация по особенностям цифрового тракта, как правило, возможна только для определения группы устройств (конкретной модели и производителя).

Результаты, полученные сотрудниками кафедры по данному направлению, используются в одном из проектов и в лабораторных работах по курсу «Технические средства защиты».

Кафедра на сегодняшний день имеет три хоздоговорных темы, одну госбюджетную тему и три гранта РФФИ общим объемом шесть миллионов рублей. Объемы НИОКР кафедры БИТ с 2001 по 2007 год приведены на рис. 2.

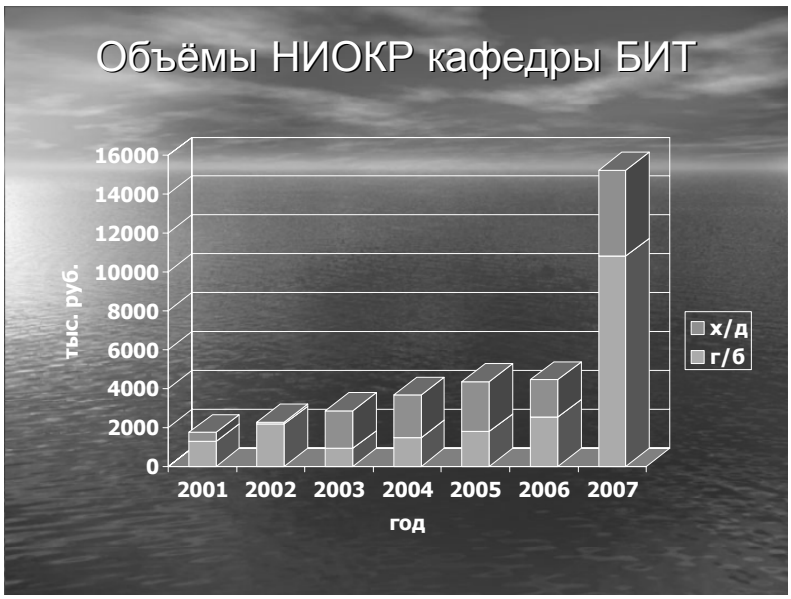

Рис. 2. Объемы НИОКР кафедры БИТ

Научные результаты НИОКР используются в учебном процессе кафедры. В 2006 г. кафедра БИТ стала дипломантом национальной отраслевой премии по безопасности «Высокие технологии общего применения в интересах национальной обороны и безопасности – ЗУБР» за полноту и качество обеспечения учебного процесса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бабенко Л.К., Макаревич О.Б.* Организация учебного процесса и научно-исследовательская работа кафедры информационной безопасности. Известия ТРТУ. Специальный выпуск / Материалы VII международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2005. №4.

2. *Бабенко Л.К., Захаревич В.Г., Макаревич О.Б.* Современные проблемы информационной безопасности и их реализация в научной и образовательной деятельности Южного федерального университета. Известия ЮФУ. Технические науки №1. Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2007. №1(76). – С. 6-9.