СЕКЦИЯ 1. ОРГАНИЗАЦИОННО–ПРАВОВОЕ И МЕТОДОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

АКТУАЛЬНЫЕ ЗАДАЧИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

В.Ф. ГОЛИКОВ

Многие важные процессы, протекающие сегодня в нашем государстве в сфере политики, экономики, безопасности, науки и техники связаны с необходимостью создания, передачи и хранения больших объёмов информации. Для решения этих задач всё шире используются современные системы, позволяющие автоматизировать работу с информационными ресурсами. Важнейшей характеристикой информационных объектов является их защищённость или в более широком смысле информационная безопасность. Обеспечение информационной безопасности объектов, как правило, комплексная проблема, включающая в себя создание правовой базы, нормативно-методических документов, комплекс организационных мер, технических средств, научно-исследовательские и опытно-конструкторские работы.

Становление системы технической защиты информации в Беларуси происходило на фоне разрыва связей с традиционными организационными и научно-техническими центрами в области информационной безопасности, оставшимися на территории Российской Федерации, а также бурного развития информационных технологий в развитых странах. Поэтому анализируемая сфера деятельности оказалась в положении постоянно догоняющей. И хотя на сегодня, благодаря существовавшему в республике научно-техническому потенциалу в области информационных технологий, некоторая часть дистанции успешно пройдена, тем не менее, проблем остаётся немало. Рассмотрим некоторые из них.

Научно-исследовательские работы. Актуальной темой исследований, на наш взгляд, остаётся исследование технических каналов утечки информации современных технических систем и средств создания обработки и передачи информации. Таких как: системы связи, автоматизированные системы управления критичными объектами, средства оргтехники и т.д. Задача этих исследований выявить реальный уровень опасности существования технических каналов. Так как недооценка их существования грозит серьёзным ущербом, связанным с утратой конфиденциальной информации, а переоценка — с ущербом за счёт неоправданных затрат на защиту. Ситуация здесь усугубляется тем, что, с одной стороны, развитие технических средств обработки информации идёт по пути снижения габаритов, материалоёмкости, потребляемой энергии, использования малоизлучающих проводников и эффективных экранов, сложных сигналов, т.е. всего того, что в конечном итоге значительно уменьшает уровень побочных электромагнитных, акустических, виброакустических, оптических и других сигналов, а также их информативность. С другой стороны, постоянно улучшаются технические характеристики разведывательной аппаратуры, увеличивается вероятность их скрытой доставки к границам объектов. Ускоряется темп смены оборудования: результаты научных исследований быстро устаревают. Все эти факторы требуют осмысления как с точки зрения системной постановки исследований, так и с точки зрения отдельных специализированных работ по электродинамике, акустике, виброакустике, оптике и т. д.

Второй крупной задачей (а по масштабам наиболее важной) являются исследования защищённости современных информационных систем, основывающихся на компьютерных сетях, от несанкционированного доступа. Здесь можно выделить следующие актуальные задачи:

Обнаружение несанкционированных действий с целью нарушения конфиденциальности, целостности и доступности информации. Обеспечение такого обнаружения основывается на использовании различных признаков: попытках обойти установленные в сети правила доступа типовыми способами, подбор паролей, резким увеличением активности действий и т. д. Правильно поставленное обнаружение атак позволит вовремя принять меры по их отражению и сохранить информационные ресурсы сети в неприкосновенности.

Аудит уязвимостей компьютерных сетей. Решение этой задачи заключается в периодической проверке безопасности системы с использованием программных или аппаратно-программных средств. При этом могут быть выявлены некорректные настройки системы безопасности, ошибки программного обеспечения, несанкционированные программные или аппаратные средства.

Исследование программных и аппаратных средств на наличие не декларированных функций. Задача "отягощается" тем, что в стране используется большое количество средств иностранного производства, поставляемых как "чёрные ящики". Наибольшую проблему здесь составляет использование операционных систем для различных вычислительных систем, являющихся "непрозрачными" для анализа. Многие страны идут по пути создания национальных операционных систем на базе свободно распространяемых типа "Linux". Республика Беларусь, на наш взгляд, располагает возможностями решения этой задачи, для этого необходимо сосредоточение усилий всех заинтересованных организаций и в первую очередь государственных в рамках некой национальной программы.

Исследования в области криптологии. Работы в этой области ведутся достаточно давно и успешно. Можно сказать, что белорусские специалисты владеют основательными теоретическими знаниями в

области построения современных криптосистем, имеют самостоятельные разработки теоретического и практического характера, что позволяет сделать вывод о том, что республика на сегодня в сфере криптотехнологий является самодостаточной.

Разработка технических средств защиты информации. Основные работы в этом направлении сводятся к разработке программных и аппаратно-программных средств, встраиваемых в существующие информационные системы. Имеется ряд изделий: по управлению доступом в компьютеры и компьютерные сети, устройства для криптографической защиты компьютерной и речевой информации, антивирусные программные средства, устройства активного зашумления, программно-аппаратные средства аутентификации пользователей и другие.

УГОЛОВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Т.В. РАДЫНО

Говоря об информационной безопасности, следует сказать: всякое государство имеет уязвимые стороны в деятельности государственных структур, коммерческих банков, предприятий, их структур, притягивающих злоумышленников. Именно поэтому развитие и распространение компьютерных систем и сетей сопровождается ростом правонарушений, связанных с кражами, злоупотреблениями, модификацией и неправомочным доступом к данным, хранящимся в памяти компьютера и передаваемых по линии связи.

В связи с вышеизложенным, в РБ получили свое развитие принципиально новые аспекты защиты информации, которые раньше не были вызваны объективной необходимостью. Одним из таких средств защиты являются меры по защите прав собственника по владению, пользованию, распоряжению и управлению информационными ресурсами. Действенным методом борьбы с хищениями путем использования компьютерной техники является включение данной новеллы в новый Уголовный кодекс Республики Беларусь. Необходимо отметить, что в правовом пространстве Российской Федерации подобного закона нет, или, иначе говоря, УК РФ 1996 г. не предусматривает подобного состава.

Непосредственным объектом данного преступления являются отношения собственности, вред которым причиняется путем хищения предмета преступления — движимого или недвижимого имущества, но чаще всего безналичных денежных средств. Объективная сторона данного преступления предполагает два варианта компьютерных манипуляций с целью обогащения за счет чужого имущества: изменение компьютерных программ, когда от каждой денежной операции осуществляется отчисление в пользу виновного: изменение номера счета одного лица на номер счета другого лица, за которым следует переадресация денег. Обычно подобная подделка осуществляется через иллюзию выборки по системе случайности.

Сложности в практике правоприменения вызывает отграничение мошенничества от хищения путем использования компьютерной техники. Ключевым моментом в такой ситуации является выяснение цели использования компьютера.

УНИВЕРСАЛЬНЫЙ КОМПЛЕКС КОЛЛЕКТИВНОГО ПОЛЬЗОВАНИЯ "ЭКЗАМЕНАЦИОННЫЙ КЛАСС — ИЗБИРАТЕЛЬНЫЙ УЧАСТОК"

В.Ю. ЛИПЕНЬ

Известен ряд систем обучения и тестирования знаний, использующих режим интерактивного взаимодействия испытуемого с обучающей системой. Вместе с тем, следует отметить, что ряд организаций, включая и Республиканский Институт контроля знаний (РИКЗ) Минобразования РБ, вынуждены использовать ручные технологии, основанные на процедурах заполнения испытуемыми опросных листов (ОЛ) и транспортировки ОЛ в уполномоченный компьютерный центр. Ручные технологии применяются и при проведении таких массовых мероприятий как опросы населения, референдумы, выборы, выдвижение кандидатов и т.п.

Построение автоматизированных систем (областных, республиканских), реализующих при приемлемых затратах указанные функции, возможно, по мнению автора, за счет использования сети недорогих универсальных пунктов опроса респондентов. Каждый из таких пунктов должен представлять собой многотерминальный (до 32 терминалов) комплекс на базе сетевого компьютера. При этом терминал респондента представляет собой простейший ручной пульт с цифровой клавиатурой и индикатором, которые служат для ввода номеров ответов. Использование большого числа дешевых терминалов, управляемых одним сетевым компьютером, позволяет осуществлять опрос большого числа респондентов и передавать через сеть данные на сервер регионального компьютерного центра для регистрации итогов единого государственного экзамена, выборов и др.