в соответствии с основными положениями Концепции национальной безопасности Республики Беларусь обеспечение необходимого уровня безопасности информационных систем и ресурсов, их целостности и конфиденциальности, основанных на применении единых требований защиты информации от несанкционированного доступа или изменения, воздействия компьютерных атак и вирусов, а также на использовании сертифицированных отечественных средств предупреждения и обнаружения компьютерных атак и защиты информации, разрабатываемых и производимых организациями, получившими в установленном порядке необходимые лицензии;

применение криптографических средств защиты информации является обязательным для информационных систем и ресурсов, содержащих сведения, составляющие служебную и государственную тайну;

централизацию и объединение конкурсов на поставку однотипной продукции для нужд органов внутренних дел, в том числе типового аппаратного, а также программного обеспечения, имеющего соответствующие лицензии, осуществляющегося в целях экономии бюджетных средств и повышения эффективности бюджетных расходов;

подготовка квалифицированных кадров органов внутренних дел на основе создания и развития информационной системы поддержки непрерывного профессионального образования, системы управления знаниями. В этих целях для обеспечения необходимого уровня квалификации сотрудников органов внутренних дел по использованию информационных технологий предлагается:

создание системы подготовки (переподготовки) кадров на основе определения требований к квалификации и навыкам использования информационных технологий для различных категорий сотрудников;

внедрение унифицированных процедур оценки квалификации сотрудников;

развитие инфраструктуры по подготовке и повышению квалификации сотрудников органов внутренних дел на базе Академии МВД Республики Беларусь;

улучшение материально-технического обеспечения, включая оснащение рабочих мест сотрудников органов внутренних дел современной вычислительной техникой:

внедрение технологий дистанционного обучения;

информирование сотрудников органов внутренних дел о передовом опыте и инновациях в сфере информационных технологий.

А.Н. Лепёхин, **А.С. Лисюк**

ПРОГРАММНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Развитие новых информационных технологий и компьютеризация управленческой деятельности привели к тому, что информационная безопасность становится не только обязательной, но и одной из характеристик информационной системы. Существует довольно обширный класс программно-технических способов защиты информации [1].

Программно-техническая подсистема комплексной защиты объектов информационной безопасности включает: физические, аппаратные, программные, аппаратно-программные, криптографические методы и средства защиты информации.

Физические средства защиты предназначены для внешней охраны территории объектов, защиты ЭВМ, систем и объектов на базе вычислительной техники. Современные физические средства защиты предоставляют широкие возможности для решения многих задач обеспечения информационной безопасности. Так, для организации охраны оборудования и перемещаемых носителей информации можно использовать:

различные замки (механические, с кодовым набором, радиоуправляемые), которые устанавливают на входные двери, сейфы, шкафы, устройства и блоки системы;

микровыключатели, фиксирующие открывание или закрывание дверей и окон;

инерционные датчики, для подключения которых можно использовать осветительную сеть, телефонные провода и проводку ТВ-антенн;

специальные наклейки из фольги или другого магнитопроводного материала, которые наклевываются на все документы, приборы, узлы и блоки системы для предотвращения их выноса из помещения.

Для нейтрализации утечки информации по электромагнитным каналам используют экранирующие и поглощающие материалы и изделия.

Для контроля электропитания могут использоваться электронные устройства-отслеживатели.

Аппаратные средства защиты – это различные электронные, электронно-механические и другие устройства, непосредственно встроенные в серийные блоки электронных систем обработки и передачи данных или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначаются для внутренней защиты структурных элементов ЭВМ, средств и систем вычислительной техники: терминалов, устройств ввода-вывода, процессоров, периферийного оборудования, линий связи и т. д.

Программные средства защиты предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в

состав программного обеспечения систем обработки данных, либо в состав средств, комплексов и систем аппаратуры контроля.

Программные средства защиты информации относятся к группе логических средств защиты и являются наиболее распространенным видом защиты, чему способствуют такие положительные свойства данных средств защиты, как универсальность, гибкость, простота реализации, возможности изменения и развития. Это обстоятельство делает их одновременно и самыми распространенными, и самыми уязвимыми элементами информационных систем.

Программно-аппаратные средства защиты связаны с совместным использованием программных и аппаратных средств защиты. Данные средства защиты широко используются при реализации биометрических методов аутентификации пользователей автоматизированных информационных систем [2].

Аутентификация – проверка идентификатора пользователя, обычно осуществляемая перед разрешением доступа к ресурсам автоматизированной информационной системы. Классификация и примеры реализации методов аутентификации, расположенных в порядке возрастания степени их надежности, представлены в таблице.

Методы аутентификации и примеры ее реализации

Метод	Пример
По знаниям (обычно используется механизм паролей)	Парольная защита Скрытые функции
По имуществу (для подтверждения своих прав необходимо предъявить системе определенный «ключ»)	Touch-memory Smart- карты
По навыкам (демонстрация отдельных умений, недоступных другим пользователям)	Клавиатурный почерк Роспись
По уникальным параметрам (сравнение каких-либо параметров человеческого тела с их цифровыми образами)	Отпечатки пальцев Сетчатка глаза Голос

Криптографические методы защиты – это методы защиты данных с помощью криптографического преобразования, под которым понимается преобразование данных шифрованием или выработкой имитовставки.

Основные криптографические методы защиты информации:

шифрование с помощью датчика псевдослучайных чисел заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы на открытые данные обратимым способом;

шифрование с помощью криптографических стандартов шифрования данных (с симметричной схемой шифрования), использующих проверенные и апробированные алгоритмы шифрования данных с хорошей криптостойкостью, например отечественный стандарт – ГОСТ 28147–89;

шифрование с помощью систем с открытым ключом, в которых для шифрования данных используется один ключ (несекретный), а для расшифрования – другой (секретный) [4].

Технические средства обеспечения информационной безопасности представляют собой большую группу различных по назначению и способам применения технических устройств.

Их в общих чертах можно подразделить на следующие категории:

программно-аппаратные средства защиты компьютерных систем и систем передачи данных;

аппаратура активной защиты от побочных электромагнитных излучений и наводок (скемблирование, шифрование);

аппаратура маскирования телефонных переговоров (специальные устройства электронной защиты телефонных аппаратов при положенной трубке, выжигатели телефонных закладных устройств) ;

средства выявления радиозакладных устройств (используются специальные средства выявления: нелинейные локаторы, индикаторы электромагнитных излучений, сканирующие приемники, системы компьютерных анализаторов);

аппаратура защиты служебных помещений от акустического, виброакустического и оптического несанкционированного снятия информации (используется специальная аппаратура, которая предназначена для борьбы со скрытоносимыми микрофонами, устройства регистрации вибрационных сигналов: устройства активного акустического зашумления помещений, устройства, основанные на способе регистрации вибрационных сигналов, стетоскопы).

Одним из актуальных аспектов программно-технической защиты автоматизированных информационных систем является *защита информации в компьютерных сетях*.

Обеспечение конфиденциальности обрабатываемой и передаваемой в сети информации, целостности и доступности ресурсов (компонентов) сети достигается с помощью специальных механизмов защиты. К их числу относятся механизмы шифрования, цифровой подписи, контроля доступа, обеспечения целостности, аутентификации, заполнения текста, управления маршрутом и освидетельствования [3].

Можно смело утверждать, что сегодня рождается новая современная технология – технология защиты информации в компьютерных информационных системах и в сетях передачи данных. Реализация этой технологии требует определенных расходов и усилий. Однако все это позволяет избежать значительно превосходящих потерь и ущерба, которые могут возникнуть при реальном осуществлении угроз информационным системам.

1. Об информации, информатизации и защите информации [Электронный ресурс]: закон Республики Беларусь от 10 ноября 2008 г. № 455-З. URL: http://www.tamby.info/zakon/zakon-455_2008.htm.

2. Девянин П.Н., Михальский О.О., Правиков Д.И., Щеобаков А.Ю. Теоретические основы компьютерной безопасности : учеб. пособие для вузов. М. : Радио и связь, 2000. 192 с.

3. Лиховидов М.В., Полещенко В.Я. Применение цифровой подписи в системах электронного документооборота // Управление защитой информации. 2004. Т. 8, № 1.

4. Шнайер Брюс. Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке С. URL: http://beda.stup.ac.ru/psf/ziss/wmaster/books/security/crypto/ 3/index.html.

П.Л. Боровик, **И.Г. Лубченок**, **Т.И. Шукайло**

ОСНОВНЫЕ НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ ТЕЛЕКОНФЕРЕНЦИЙ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Повышение эффективности использования времени и ресурсов становится превалирующим фактором развития современного общества. Не осталась в стороне и система правоохранительных органов Республики Беларусь. Увеличение количества рассматриваемых уголовных дел, сокращение сроков их рассмотрения, необходимость жесткой экономии времени и средств на передвижение, а также объективная потребность в оперативном доступе к информации обусловливают востребованность технологии, которая позволяет видеть и слышать друг друга на расстоянии, обмениваться данными и совместно их обрабатывать в реальном режиме времени.

Идеальным инструментом, обладающим необходимыми функциональными возможностями и позволяющим реализовать вышеуказанные запросы, является технология видеоконференцсвязи (ВКС).

Анализируя литературу, посвященную данной проблематике, можно отметить, что вышеуказанные системы давно нашли широкое применение (преимущественно за рубежом) в крупных компаниях, юридических фирмах, в сфере здравоохранения и во многих других областях. Управление и бизнес, дистанционное обучение, телемедицина, подбор персонала при приеме на работу, оперативный контроль и безопасность – лишь малая часть тех областей деятельности, где преимущества ВКС совершенно очевидны.

Кроме того, современные средства ВКС предоставляют возможности для совместной работы с данными и различными приложениями, вплоть до подписания документов, а существующие средства криптозащиты позволяют сохранить конфиденциальность содержания сеансов видеосвязи.

В этой связи примечателен опыт использования ВКС в уголовно-исполнительной системе Российской Федерации, где внедрена система

многоточечных видеоконференций. Последние позволяют рассматривать дела с участием нескольких следственных изоляторов как Москвы, так и субъектов Российской Федерации единовременно. Данная технология обеспечивает дистанционное общение всех участников судебного заседания в режиме реального времени, снимая необходимость этапирования подследственных в зал суда.

Применение телекоммуникационных технологий позволяет также проводить опросы свидетелей по уголовному или иному судебному делопроизводству с искажением их голоса и сокрытием лица в соответствии с российскими и международными правовыми актами по защите свидетелей. Кроме того, использование ВКС позволяет сократить сроки рассмотрения дел и повысить эффективность судопроизводства, поскольку несвоевременная явка свидетелей – одна из основных причин затягивания судебных процессов. Причем опыт использования видеосвязи при допросах в Российской Федерации уже имеется: сейчас с ее применением рассматривают кассационные жалобы по уголовным делам.

Кроме ВКС для непосредственного исполнения судебных функций система широко используется для организации консультаций, совещаний, семинаров судей и сотрудников аппарата суда с коллегами из одного или нескольких судов. Заслуживает внимания и интерактивное дистанционное обучение сотрудников судов общей юрисдикции и исправительных учреждений Федеральной службы исполнения наказаний России использованию видеотехнологий при проведении судебных процессов.

Как показывает мировой опыт, наиболее широко ВКС в судопроизводстве применяется в судебно-пенитенциарной системе – в основном для заслушивания свидетельских показаний и общения осужденных с адвокатами и родственниками. Однако непосредственно для проведения судебных заседаний технология ВКС была впервые применена в России. В настоящее время в Верховном Суде Российской Федерации проходит до 100 сеансов видеоконференцсвязи в день и уже проведено более 170 тыс. сеансов. Кроме того, по данной технологии работает более 90 судов общей юрисдикции областного уровня.

Принимая во внимание вышесказанное, нельзя не отметить, что и в деятельности органов внутренних дел Республики Беларусь существует несколько сегментов, где особенно востребована технология ВКС.

В соответствии с ч. 3 ст. 68 Уголовно-процессуального кодекса Республики Беларусь с использованием видеотехнических средств может быть произведен допрос защищаемого лица при нахождении его вне зала судебного заседания. В этом случае суду, который находится по месту пребывания свидетеля, дается поручение организовать до-