– ограничить доступ к информации и обеспечить персональную ответственность за ее сохранность;

– обеспечить допуск к ответственным объектам только сертифицированных специалистов;

– избежать накладных расходов, связанных с эксплуатацией систем контроля доступа (карты, ключи);

– исключить неудобства, связанные с утерей, порчей или элементарным забыванием ключей, карт, паролей;

– организовать учет доступа и посещаемости сотрудников.

При необходимости выделить конкретного человека из толпы, и установить его личность, не существует системы, которая справилась бы лучше, чем распознавание по лицу. Существенным преимуществом распознавания данным методом перед другими биометрическими методами является возможность идентификации на расстоянии. Это значит, что идентифицировать человека можно без его ведома.

Разработана система распознавания изображений лица с помощью метода главных компонент. Данная программа позволяет привнести в учебный процесс понимание принципов работы систем биометрической идентификации. В достоверности полученных теоретических знаний, можно убедиться на практике, сделав выводы из результатов полученных в ходе работы с программой. Это является несомненным плюсом, при подготовке специалистов в области информационной безопасности.

Очевидно, что в ближайшие несколько лет, учитывая появление всё более дешевого и высокопроизводительного оборудования, а также всё более возрастающие потребности в быстрой и своевременной идентификации личности, применение биометрических систем распознавания станет общераспространенным.

РАЗРАБОТКА МЕТОДОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОСНОВЫ СОЗДАНИЯ И ИЗУЧЕНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

В.Ф. ГОЛИКОВ, И.И. ЧЕРНАЯ, О.Б. ЗЕЛЬМАНСКИЙ

Проблема защиты информации в сегодняшнем обществе — это многогранная проблема сохранения важнейшего ресурса этого общества — информационного ресурса.

Поэтому вопрос изучения и создания методологических основ информационной безопасности является чрезвычайно актуальным.

В докладе предлагается концепция методологии информационной безопасности, базирующаяся на основных законах, регламентирующих юридические аспекты обеспечения безопасности информации и международном опыте создания защищенных систем. Основные принципы функционирования подобных систем и технология их создания, а также исследования и изучения их невозможны без регламентации основных понятий и концепций информационной безопасности на государственном и международном уровне посредством стандартизации требований и критериев безопасности, образующих шкалу оценки степени защищенности.

В докладе рассмотрены методологические аспекты систем обеспечения информационной безопасности, включающие терминологию, общую модель и общие критерии оценки безопасности информационных изделий. Приводятся также основные классы функциональных требований безопасности и требования доверия безопасности на всех этапах разработки и эксплуатации изделий.

Материалы доклада успешно опробованы при проведении лекционных и практических занятий с магистрантами.