спектр навыков — от монтажа приборов и аппаратуры автоматического контроля и управления, ее наладки и технического обслуживания до запуска программных систем управления доступом и средствами охранной сигнализации и видеонаблюдения.

Современные системы рассматриваемого класса выполняются как сетевые с реализацией многопользовательских режимов IP-видеонаблюдения, обеспечивающих выполнение различных функций в online-режиме с использованием веб-интерфейсов. С учетом этого, учебные лаборатории должны реализовываться на основе локальных вычислительных сетей, имеющих выход на серверное оборудование с соответствующим программным обеспечением.

Очень важным является наличие в лаборатории оборудования с поддержкой технологий беспроводной передачи информации и облачных сервисов, так как данные технологии широко используются в последнее время в оборудовании охраны и видеонаблюдения.

Таким образом, современная лаборатория для подготовки специалистов, эксплуатирующих системы охраны и видеонаблюдения должна не просто включать достаточно широкий набор отдельных технических средств охраны радиолучевого, проводного, сейсмического, вибросейсмического и других типов (с учетом номенклатуры применяемых, выпускаемых и перспективных изделий), но и поддерживать современные телекоммуникационные и информационные технологии обработки данных.

Только такой подход обеспечит изучение современных систем безопасности как интегрированного централизованно управляемого комплекса оборудования, использующего общие линии связи и базы данных и обеспечивающего эффективное взаимодействие индивидуальных подсистем, входящих в его состав.

СИСТЕМА РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ ЛИЦА ДЛЯ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ «БИОМЕТРИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Р.В. РАБЦЕВИЧ, А.М. ПРУДНИК

Стремительное развитие информационных технологий с несомненными удобствами привело к появлению новых видов мошенничества и киберпреступлений. Крайне важно, чтобы от быстро развивающихся информационных технологий не отставала и безопасность.

В настоящее время приобретают широкое распространение биометрические технологии автоматической аутентификации и идентификации личности. Это обусловлено множеством причин. Из-за быстрого развития сектора электронной коммерции значительно возросли требования к защищенности информационных ресурсов. Установление личности человека по изображению лица, может быть дополнительной мерой защиты наряду с паролем, ключом.

Применение биометрических систем распознавания, решает такие важные задачи как, аутентификация, контроль доступа, невозможность отказа от авторства. Биометрические системы идентификации человека по изображению лица, могут использоваться не только для поиска людей, преступников, но могут вознести на новый уровень контроль физического доступа к объекту. Если говорить о 3d распознавании, то вероятность ложной идентификации (FAR), то есть вероятность того, что система по ошибке признает подлинность пользователя, не зарегистрированного в системе, крайне мала. Что позволяет уже сейчас использовать данные системы в местах, где требуется самый серьезный уровень защищенности.

Диапазон проблем, решение которых может быть найдено с использованием системы контроля и управления доступом на основе распознавания лица:

– предотвратить проникновение злоумышленников на охраняемые территории и в помещения за счет подделки, кражи документов, карт, паролей;

– 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.