возможности эффективного распознавания ладони при анализе видеопотока камеры [1]. Это позволяет использовать цифровые камеры для получения информации о пользователе компьютера. Также в работе Бакиной И.Г. приводятся алгоритмы распознавания исключающие ошибки «склеивания пальцев» и длинных ногтей [2].

В настоящее время крупные производители компьютерной техники выпустили прототипы программного обеспечения для авторизации в системе ноутбуков. Среди них самые примечательные образцы: VeriFace от компании Lenovo, Face Recognition от Toshiba и SmartLogon от Asus. К сожалению, в алгоритмах этих программ заложены функции сравнения получаемого от камеры изображения лица с заданным образцом. Здесь высока вероятность ложного доступа в систему по представлению распечатанного изображения пользователя. Попытки устранения этой уязвимости предприняла компания NeuroTechnology в своем продукте VeriLook. Предпринятые попытки обмануть систему фотографией не увенчались успехом. Данный факт позволяет утверждать: а) технология биометрического распознавания пользователей по фото веб-камеры имеет перспективы развития; б) методика распознавания требует значительных доработок для повышения эффективности.

Литература

1. Нгуен Тоан Тханг. Алгоритмическое и программное обеспечение для распознавания формы руки в реальном времени с использованием SURF-дескрипторов и нейронной сети / Нгуен Тоан Тханг, В.Г. Спицын // Известия Томского политехнического университета. – 2012. – № 5 (320).

2. Бакина, И.Г. Генерация признаков для сравнения ладоней при наличии артефактов / И.Г. Бакина // Журнал «Прикладная информатика». – 2009. – № 4 (22).

ЧИСЛЕННОЕ ОПРЕДЕЛЕНИЕ РИСКОВ БЕЗОПАСНОСТИ СВЯЗИ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.В. Макатерчик

В настоящее время значительно возрастает роль современных инфокоммуникационных систем специального назначения (ИКС СН). Развитие и совершенствование таких систем ведется в соответствии с общемировыми тенденциями. Активное внедрение новых средств связи, протоколов и инфокоммуникационных технологий привело к появлению неизученных угроз безопасности связи, возможность реализации которых злоумышленниками негативно влияет на обеспечение информационной безопасности государства и организаций различных форм собственности. Под угрозой безопасности связи понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба системе связи или ее компонентам.

Выделяют следующие виды возможных атак на ИКС СН: пассивная, активная (отказ в обслуживании, модификация потока, создание ложного потока, повторное использование). При этом реализация атаки на ИКС СН включает следующие этапы: сбор информации, выбор метода реализации и типа атаки, реализация выбранного типа атаки, завершение атаки.

На основе проведенного анализа реализации угроз информационной безопасности численное определение рисков безопасности связи для элемента ИКС СН определен способ численного определения рисков безопасности связи для элемента инфокоммуникационных систем специального назначения использованием выведенной формулы. Полученные для каждого элемента ИКС СН значения в дальнейшем используются в ходе определения численного значения рисков безопасности связи для всей ИКС СН. Предложенный подход позволяет определить численное значение рисков безопасности связи для ИКС СН с учетом как существующих, так и потенциальных уязвимостей на основе оценки мероприятий по обеспечению безопасности связи.

Библиотека БГУИР