Также предлагается метод идентификации пользователей по «клавиатурному почерку», основанный на применении статистических критериев. Данный метод обладает рядом положительных особенностей:

- высокая надежность идентификации,
- простота реализации,
- независимость от языка, на котором осуществляется ввод текста,
- нечувствительность к аппаратной составляющей системы,
- возможность идентификации пользователя по произвольному тексту,
- отсутствие необходимости в предварительном обучении системы, достаточно создания только одного контрольного образа для каждого пользователя.

СПИСОК ЛИТЕРАТУРЫ:

1. *Трушина Е. А.* Идентификация пользователя ЭВМ по клавиатурному почерку как метод защиты от несанкционированного доступа. 1997. //Электронный источник, опубликовано на сайте http://www.securityclub.ru/
2. *Иванов А. И.* Нейросетевые алгоритмы биометрической идентификации личности / Научная серия «Нейрокомпьютеры и их применение». Кн. 15. Ред. А. И. Галушкин. М.: Радиотехника, 2004. — 143 с.
3. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

А. Н. Ручай

ПРОТОТИП ЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА НА ОСНОВЕ ИЗБИРАТЕЛЬНОЙ МНОГОФАКТОРНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Разработчики и исследователи биометрических систем предлагают программные реализации на основе, как правило, только одной биометрической характеристики без дополнительных инструментов и модулей, что создает проблемы при их использовании и эксплуатации [1].

В зависимости от разных условий и факторов, в частности от доступности электронных средств, удобства, стойкости к атакам и уязвимостям, болезней или увечий пользователей, может быть выбрана биометрическая аутентификация на основе любых таких биометрических характеристик, как ритм ввода пароля, голос, динамика подписи и графическое распознавание. Например, если необходимо разграничить права доступа в изолированном помещении без посторонних, то может быть использована аутентификация по голосу, по ритму ввода пароля или графическому распознаванию. Если помещение, наоборот, не обладает такими условиями, то аутентификация может быть осуществлена на основе ритма ввода пароля или по динамике подписи. Для осуществления аутентификации в мобильных или сенсорных устройствах может быть выбрана аутентификация по ритму ввода пароля, по динамике подписи или графическому распознаванию. На пропускных пунктах возможна аутентификация по динамике подписи.

В настоящее время актуальной является задача разработки универсальных модулей, реализующих разграничение прав доступа на основе биометрической аутентификации [2]. Данная

задача своевременна и интересна, замыкается на вопросах государственной безопасности и входит в концепцию развития Российской академии наук [1]. Кроме того, системы разграничения доступа на основе биометрической аутентификации имеют большую практическую значимость и преимущества: уникальность, неотъемлемость и неотчуждаемость биометрической характеристики; затруднения при проведении атаки подбора по биометрической характеристике; независимость от операционной системы и кодировок символов; избирательность и многофакторность аутентификации; отсутствие ошибок третьего рода, когда невозможно аутентифицировать человека из-за болезней и увечий.

Задачей данного проекта была разработка, исследование и реализация прототипа централизованной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации с клиент-серверной архитектурой. Для этого необходимо было решить следующие задачи: разработка принципов построения системы, архитектуры, протокола взаимодействия; разработка и реализация центра и модулей биометрической аутентификации; оценка надежности и тестирование работы модулей аутентификации по различным биометрическим характеристикам на собранных биометрических базах.

На основе анализа модели существующих атак и защиты можно сделать вывод, что многие проблемы и атаки предотвращаются с помощью цифрового кодирования, временных меток и шифрования открытого канала передачи данных [3]. В связи с этим система разграничения прав доступа должна быть реализована с клиент-серверной архитектурой, что дает следующие преимущества: повышается общая безопасность системы; один мощный сервер сможет одновременно обслуживать множество клиентов; обеспечивается минимальная нагрузка на компьютер клиента; сводится к минимуму количество клиентских настроек; сервер можно переносить под любую ОС, а клиентские части останутся неизменными; клиентскую часть также можно написать под другую ОС, а сервер останется неизменным.

На устройствах устанавливаются специализированные модули биометрической аутентификации, считывающие информацию пользователя и передающие запросы в единый центр. Задачами центра являются хранение информации биометрической аутентификации и обработка запросов аутентификации.

Для защиты данных, передаваемых между модулями и центром, в рамках протокола передачи биометрической информации создается защищенный канал связи с использованием криптографической защиты. В модулях устройств были реализованы на системном уровне методы, противодействующие несанкционированному отключению модуля аутентификации, а также снижающие риск негативных воздействий на него, приводящих к снижению безопасности системы в целом.

В едином центре аутентификации была реализована эффективная и защищенная система хранения базы зарегистрированных биометрических данных, которая должна работать достаточно быстро, а также исключать возможность несанкционированного доступа, модификации, уничтожения и блокирования данных. Помимо этого, в центре была реализована подсистема аудита событий безопасности и политика разграничения доступа пользователей.

Важным при разработке централизованной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации было соблюдение действующих российских стандартов в сфере биометрических технологий.

СПИСОК ЛИТЕРАТУРЫ:

1. *Ручай А. Н.* Текстозависимая верификация диктора: математическая модель, статистические исследования, комплекс программ. Saarbrücken: LAP LAMBERT Academic Publishing, 2012. — 144 с.

2. *Ручай А. Н.* Разработка комплекса модулей для разграничения прав доступа в ОС Windows XP на основе биометрической аутентификации // Информационные технологии и системы: материалы Первой Международной конференции. Челябинск: ЧелГУ, 2012. С. 75–76.
3. *Ручай А. Н.* Модель атак и защиты на биометрическую систему распознавания диктора // Доклады ТУСУР. 2011. № 1 (23). С. 96–100.

А. Ю. Сенцова, И. В. Машкина

АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

В настоящее время все большее распространение получает *технология облачных вычислений*, при которой данные, программное обеспечение (ПО), прикладные системы, компьютерные ресурсы предоставляются клиентам по запросу как услуга через Интернет [1]. При этом заказчик имеет тот уровень защищенности в облаке, который обеспечивается вендором, поэтому существует необходимость анализа и оценки возможных информационных рисков в системе облачных вычислений (СОбВ).

Облачная модель состоит из сервисов клиентов, управляемого централизованного контента и виртуальной инфраструктуры. Кроме таких компонентов традиционной инфраструктуры информационной системы, как сеть, компьютеры, серверы, в архитектуру облачной системы входят blade-сервер и облачные приложения [2].

В работе рассматривается бизнес-модель продажи и использования *приложения как услуги (SaaS)*. Вендор в этом случае разрабатывает веб-приложение и предоставляет заказчику (клиенту) доступ к ПО через Интернет. На основе анализа технологии клиент-серверного взаимодействия и известных описаний существующих систем разработана *архитектура облачной системы*. Архитектура системы облачных вычислений настолько сложна, что она приобретает новые, неизвестные прежде уязвимости. Переход к облачным средам приводит к появлению *принципиально новых угроз* [3]. Для облачных сред угрозы удаленного взлома и заражения вредоносным кодом весьма значимы из-за параллельного существования множества виртуальных машин. Кроме того, виртуальная машина отличается от физической возможностью ее заражения в *выключенном* состоянии [1, 3], если есть доступ к хранилищу образов виртуальных машин через сеть. Поэтому особое внимание должно быть уделено *политикам безопасности* в виртуальных инфраструктурах.

Опасность возникновения ущерба или убытков в результате использования организацией облачных сред может быть оценена величиной информационного риска в системе облачных вычислений. В данной работе предложена концептуальная модель угроз в виде *нечетких когнитивных карт* (НКК), построенных на основе разработанной системы облачных вычислений, для анализа рисков нарушения информационной безопасности.

Информационный риск обусловлен наличием угроз нарушения безопасности информации. Поэтому необходимо в первую очередь идентифицировать все возможные угрозы и их источники. Каждая угроза должна быть детализирована и оценена с учетом наличия уязвимостей на путях ее распространения.

Применение НКК позволяет произвести моделирование процессов распространения угроз в системе облачных вычислений через используемые уязвимости компонентов ее архитектуры. При этом полученная модель обладает свойством *наглядности*, простотой *понимания и перевода* содержательного знания эксперта на математический язык.