Таким образом можно сделать вывод, что предложенный алгоритм уверенно идентифицирует наблюдаемые субъекты. Платой за возможность идентификации является увеличение времени принятия решения до нескольких измерений.

При малых различиях вычисляемых параметров работа идентификатора определяется достоверностью знания априорных законов распределения для заданных субъектов. Принять решение о возможности использования данного алгоритма возможно только после получения достаточного количества полных и достоверных экспериментальных данных о биометрических параметрах субъектов идентификации в различных условиях.

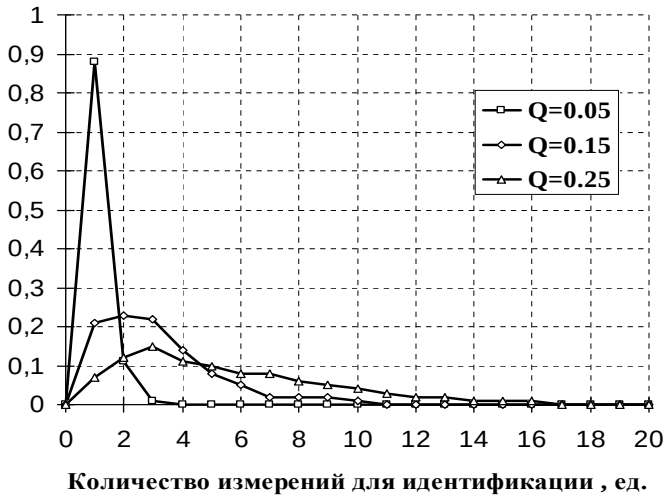

Рис.2. Закон распределения числа измерений, необходимых для идентификации субъекта

Литература

1. Бухалев, В. А. Распознавание, оценивание и управление в системах со случайной скачкообразной структурой. – М. : Наука, 1996 .

2. Алгоритм распознавания состояния программы на основе систем со случайной структурой Перспективные информационные технологии (ПИТ 2014): труды Международной научно-технической конференции Самара: Издательство Самарского научного центра РАН, 2014.

3. Прохоров С.А. Аппроксимативный анализ случайных процессов. – 2-е изд., перераб. и доп./СНЦ РАН, 2001.

А.Н. Мазалов

ЗАЩИЩЕННАЯ ДВУХФАКТОРНАЯ ГРАФИЧЕСКАЯ АУТЕНТИФИКАЦИЯ В СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

(Тамбовский государственный технический университет)

В настоящее время развития рынка систем контроля и управления доступом (СКУД) однозначно направлено на снижение влияния человеческого фактора на процесс обеспечения пропускного режима на объектах. Это повлияло на развитие систем использующих многофакторную аутентификацию.

Использование СКУД позволяет предотвратить несанкционированный доступ людей, транспорта и других объектов в зону (из зоны) доступа в целях обеспечения противокриминальной защиты. [2]

Одним из главных и уязвимых элементов СКУД является идентификатор пользователя. Злоумышленник, скомпрометировав статичный идентификатор, может воспользоваться большим потоком посетителей и пройти через контрольно-пропускной пункт как легальный пользователь. Следовательно, перед специалистами встает задача создания современного защищенного идентификатора.

В настоящее время в качестве идентификаторов применяются такие технологии, как бесконтактные радиочастотные карты и метки, магнитные карты, touch-memory, карты Виганда, штрих-кодовые линейные и многомерные метки. [1]

При проведении исследований мною были проанализированы существующие на сегодняшний день технологии (рис. 1). Анализ данных технологий показал, что идентификаторы, выполненные по технологии QR-кодов обладают существенными преимуществами по сравнению с остальными. Данные идентификаторы имеют минимальную стоимость, не подвержены помехам в виде электромагнитных полей, что является существенной проблемой RFID-технологии, могут работать при повреждениях метки.

Для исправления ошибок в QR-кодах применяется код Рида-Соломона с 8-битным кодовым словом. Существует четыре уровня избыточности: 7, 15, 25 и 30 %. Благодаря исправлению ошибок, удаётся считать код даже если он поврежден на 30%, что является невозможным при работе с его аналогами. [3]

Одним из недостатков QR – кодов является возможность их подделки, так как сам QR-код непосредственно не защищен. В данной работе, предлагается новый метод, который позволяет этого избежать.

Защита идентификатора пользователя будет осуществляться следующим способом.

Характеристика	RFID	Штрих-код	QR-код
Необходимость в прямой видимости	Возможно чтение без прямого контакта и вне зоны видимости	Чтение без прямой видимости невозможно	Чтение без прямой видимости невозможно
Объём памяти	От 10 до 512 000 байт	До 100 байт	До 3 072 байт
Дальность регистрации	До 300 м	До 4 м	До 1 м
Возможность перезаписи данных и многократного использования метки	Нет / Есть	Нет	Нет
Безопасность и защита от подделки	Подделка практически невозможна	Подделать легко	Подделать возможно
Работа при повреждении метки	Невозможна	Затруднена	Возможна
Подверженность помехам в виде электромагнитных полей	Есть	Нет	Нет
Стоимость	Средняя и высокая	Низкая	Низкая

Рис. 1 – Сравнительный анализ RFID, штрих-код и QR-код технологий

Лицевая сторона пропуска (рис. 2) содержит идентификационные признаки организации и QR1-код, содержащий идентификатор (ID) пользователя.

Рис. 2 – Лицевая сторона (слева), оборотная сторона пропуска в видимом (справа) и инфракрасном диапазоне (нижняя)

На оборотной стороне пропуска обнаружить какую-либо информацию в видимом диапазоне невозможно. Однако, если просканировать ее в инфракрасном диапазоне, то мы увидим второй QR2-код, защищающий пропуск от подделки.

Защитный QR2-код наносится на пропуск специальными инфракрасными чернилами при помощи принтера. Он будет нести в себе значения SALT и Hash(PIN) карты, которые являются уникальными для каждого пропуска. По сути, это специальная информация для подтверждения подлинности карты в СКУД.

Аутентификация пользователя в СКУД будет осуществляться при помощи вычисления значения хеш-функции от двух QR-кодов, однако из QR2 будет браться не оба значения, а только SALT карты.

$$QR1 + QR2 \rightarrow hash(ID + SALT)$$

В результате сравнения значения Hash(ID + SALT) со значением Hash*(ID + SALT), хранящемся в базе данных сервера, выдается результат аутентификации – разрешение или запрет на вход в контролируемую зону.

Алгоритм работы

Для работы в системе пользователю необходимо быть зарегистрированном в базе данных (БД) организации. Внесение пользовательских данных в БД

проводит администратор системы. После этого зарегистрированный пользователь может быть распознан.

В начале работы системы необходимо поднести идентификатор пользователя к устройству считывателя. Произойдет считывание двух QR-кодов с разных сторон идентификатора. В результате чего, из QR1 будет получен идентификатор (ID) пользователя, а из QR2 будет извлечены SALT и Hash(PIN) карты.

При работе системы в штатном режиме на сервер отправляется запрос прохождения процедуры аутентификации. В этом запросе на сервер посылается Hash-карты, сформированный путем сложения ID пользователя, извлеченного из QR1 и SALT, извлеченной из QR2.

Сервер проверяет данные полученные с терминала, с данными, хранящимися в БД.

После процедуры проверки сервер посылает ответ, разрешающий или запрещающий доступ субъекту на контролируемую территорию.

При возникновении неполадок в сети, то есть, когда отправить запрос на сервер не представляется возможным, начинает функционировать второй режим работы системы.

Пользователь предъявляет свой идентификатор. Система, зная, что не может отправить запрос на сервер, просит субъект ввести PIN, который может быть известен только законному пользователю системы.

Терминал вычисляет значение хеш от PIN, введенного пользователем. После этого сравнивает его со значением Hash(PIN), хранящемся в QR2-коде карты. Терминалом выдается результат аутентификации – разрешение или запрет на вход в контролируемую зону.

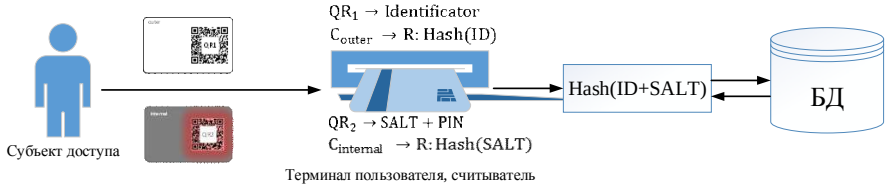

Рис. 3 – Фрагмент структурной схемы алгоритма СКУД на основе двухфакторной графической аутентификации

Подделка идентификатора

В случае утери идентификатора легальный пользователь системы должен сообщить об этом в службу безопасности, которая, в свою очередь, вводит в действие второй режим работы системы, при котором во время прохождения процедуры аутентификации необходимо вводить PIN-код.

Злоумышленник может украсть идентификатор и воспользоваться им при прохождении на объект, предоставив его системе. В данном случае, злоумышленник не знает о наличии на оборотной стороне идентификатора дополнительного невидимого QR-кода и не сможет попасть на контролируемую территорию.

Система, находясь во втором режиме работы, попросит субъект ввести PIN-код, который известен только законному пользователю. Нарушитель, попытавшись ввести его, получит отказ.

Возможности использования

Изготовление идентификаторов выполненных по данной технологии является несложным и быстрым процессом. Такие идентификаторы можно напечатать на любом принтере, лишь заменив в нем чернила на инфракрасные.

Перспективным решением является использование данных идентификаторов в качестве одноразовых пропусков на объектах с зонами ограниченного доступа. Контролер может выдавать одноразовые пропуска субъектам запросившим их. В данном случае, субъекту необходимо предоставить свои паспортные данные и сообщить цель визита на объект.

СКУД на основе двухфакторной графической аутентификации применимы во всех организациях, где присутствует необходимость контроля доступа на охраняемую территорию или в зону ограниченного доступа. К таким объектам можно отнести учреждения образования, здравоохранения, транспорта, бизнеса, культуры, жилищно-коммунального хозяйства.

Вывод

В рамках разработки системы двухфакторной графической аутентификации был предложен подход, заключающийся в использовании в качестве идентификатора субъекта технологии QR-кодов. Данная технология позволяет защитить пропуск от подделки, прилагая при этом минимум материальных, физических и финансовых затрат.

Отличительной особенностью подхода является применение на идентификаторе двух QR-кодов, нанесенных на разные стороны пропуска. Защитный QR-код, нанесенный на оборотную сторону является невидимым в обычном (видимом) диапазоне, что позволяет защитить идентификатор от подделки. Данный QR-код возможно считать только в инфракрасном диапазоне.

Предлагаемый подход позволяет не только повысить степень защищенности идентификатора, но и решить проблему стоимости внедрения СКУД, так как является более дешевым.

Литература

1. Ворона В. А. Системы контроля и управления доступом / Ворона В. А., Тихонов В. А. – М.: Горячая линия-Телеком, 2010. - 272 с.

2. Шелупанова А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А.А. Шелупанова [и др.]. – М.: Горячая линия-Телеком, 2012. – 550 с.

3. QR код [Электронный ресурс]. – Режим доступа: http://www.qrcc.ru/qrcode.html

4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/ В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.

5. Громов Ю.Ю., Тихомирова А.А., Щербинин П.А, Яковлев А.В. Двумерный штрихкод как идентифицирующая метка в системах контроля и управления доступом // «Известия академии инженерных наук им. А.М. Прохорова»: ежеквартальный научно-технический журнал. – М.: Научтехлитиздат, 2013, №1

В.О. Рублевская, В.А. Акулов

ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ КЛАСТЕРИЗАЦИИ ОБЪЕКТОВ: АЛГОРИТМЫ И ПРОГРАММНЫЕ СРЕДСТВА

(Самарский государственный технический университет)

Актуальность и цели.

Объектом исследования являются алгоритмы кластеризации сложных объектов на геоинформационных картах, а так же ограничение доступа к ним [1],[2]. Предметом исследования являлась разработка новых алгоритмов на основе объединения объектов по расстоянию с использованием графов и окружностей.

Цель исследования: разработка программного средства, предназначенного для управления доступом к кластеризованым объектам.

Материалы и методы.

В качестве основного метода защиты информации применено имитационное моделирование. Предусмотрено отображение карт и кластеров на их поверхности с использованием средств библиотеки CesiumJS. Выполнена оценка быстродействия системы.

Результаты.

Решена задача кластеризации групп объектов с использованием графов и окружностей. Каждый из этих способов предусматривает наличие системы безопасности, которая отображает кластеризацию лишь на тех уровнях, которые доступны для просмотра пользователю. Уровень доступа напрямую связан с масштабированием ландшафтной сетки. В общей сложности предусмотрено 25 градаций, что, в свою очередь, обеспечивает высокую гибкость системы и адаптацию к конкретным условиям.