8. Возможность работы при нестабильной связи между различными филиалами организации.

Ввиду того, что репликация происходит не в режиме реального времени, при её работе возможно появление логических ошибок, когда с двух различных участников репликации происходит редактирование одного и того же пропуска. После проведения репликации они обмениваются своими изменениями, и значения перестают быть одинаковыми. Такие ошибки являются трудоемкими для обнаружения, т.к. формально процедура репликации завершилась успешно, а по факту – нет. Для того, чтобы максимально сократить вероятность появления таких ошибок используется правило, что данные в Центре имеют более высокий приоритет, чем в филиале. Данное правило также будет работать в случае, если происходит одновременное редактирование данных в двух разных филиалах, т.к. репликация осуществляется транзитом через Центральный офис.

9. Обеспечение защищенной передачи данных

Для безопасного соединения удаленных серверов баз данных между собой рекомендуется организации VPN-соединения. Для дополнительной защиты информации данные промежуточных таблиц могут шифроваться любым современным алгоритмом шифрования, как симметричным, так и асимметричным. Проблема передачи ключей для расшифровки информации в данном случае не стоит, так как информация реплицируется внутри одной, пусть и распределенной организации.

Опыт внедрения полученной системы репликации свидетельствует о том, что все заявленные цели, поставленные при ее проектировании, были достигнуты. В настоящее время ведется мониторинг возможных конфликтов репликации с тем, чтобы предложить пользователям автоматические средства по их разрешению.

Литература

1. Kirtikumar Deshpande. Oracle Streams 11g Data Replication. - McGraw-Hill Osborne Media, 2011. – 546 с.

2. Базилевский Е.В. Альтернативный способ разрешения конфликтов репликации в распределенных базах данных Oracle // Современные проблемы науки и образования. - 2012. №2. - С. 266

3. Гришмановский П.В., Базилевский Е.В. Анализ технологий репликации данных и методы повышения эффективности разрешения конфликтов репликации // Вестник Волжского университета им. В.Н. Татищева. - 2012. №2[19]. - С. 98-106

4. B. Prusinski, S. Phillips, R. Chung. Expert Oracle GoldenGate. - Apress, 2011. – 352 с.

5. Крутов А.Н. Разработка защищенной системы репликации // Информационное противодействие угрозам терроризма, 2015, №24, С. 81-85

А.Б. Кузьмичев

АЛГОРИТМ ИДЕНТИФИКАЦИИ СУБЪЕКТА ПО БИОМЕТРИЧЕСКИМ ПРИЗНАКАМ НА ОСНОВЕ ТЕОРИИ СИСТЕМ СО СЛУЧАЙНОЙ СТРУКТУРОЙ

(Тольяттинский государственный университет, г. о. Тольятти)

Идентификация субъекта по биометрическим признакам возможно реализовать при различиях в параметрах, которые можно измерить по характеристикам, присущих человеку. Такими параметрами могут являться такие как лицо, голос, отпечатки пальцев, клавиатурный почерк и т.д. В основе идентификации лежит вычисление выбранных биометрических параметров χ на основе измерений по идентифицируемому субъекту, и сравнение их на степень совпадения с априорно известными или измеренными ранее биометрическими параметрами по выбранным субъектам. При малых различиях вычисляемых параметров и наличии ошибок в оценке измерений по идентифицируемым субъектам, увеличивается вероятность принятия ошибочного решения $P_{o\text{р}}$ при простом сравнении полученной оценки параметра с некоторой границей принятия решения. Одним из путей уменьшения $P_{o\text{р}}$ является увеличение количества измерений χ и их усреднении с целью уменьшения ошибки в оценке выбранного параметра.

В данной работе предлагается использовать алгоритма идентификатора, построенного с применением теории систем со случайно изменяющейся структурой. Данный алгоритм по известным законам распределения биометрических параметров для субъектов идентификации позволяет оценить вероятность того, что данный субъект является требуемым субъектом идентификации. Рассмотрим в качестве примера алгоритм идентификации субъекта по одному измеряемому биометрическому параметру. Для этого используем математический аппарат, предложенный в [1] и рассмотренный в [2].

Постановка задачи. Имеются априорные данные о распределении биометрического параметра для вероятных субъектов, подлежащих идентификации. В процессе измерений от *m* обнаруженных субъектов производятся вычисления биометрических параметров χ_{j} (j=1,m) с ошибкой, априорно известной исходя из конкретного типа измерителей характеристик человека и их условий применения.

Принятые допущения:

1. Уравнения объекта имеют вид :

$$\dot{\chi} = 0\,,$$

$$\chi(0) = \chi_0\ ,\ \chi_0 = \mathrm{N}_{\text{усеч}}\{m_x(s_k), \sigma_x(s_k)\}, \quad (1)$$

где $m_x(s_k), \sigma_x(s_k)$ - математическое ожидание и СКО распределения априорных данных в состоянии s_k.

2. Вероятность перехода в состояние отличное от исходного равна нулю:

$$q(s_{k+1}|s_k) = 0 \text{ , для } s_{k+1} \neq s_k \text{ ,}$$
$$q(s_{k+1}|s_k) = 1 \text{ , для } s_{k+1} = s_k \text{ ,} \qquad (2)$$

3. Отсутствуют индикаторы смены состояния.

Для синтеза алгоритма идентификации примем состояния, которые может принимать субъекты:

1 – субъект с параметрами класса A_1 ;

2 - субъект с параметрами класса A_2 ;

d - субъект с параметрами класса A_d.

При принятых допущениях уравнения алгоритма [2] примут следующий вид:

$$p_j(s_{k+1}) = \vartheta_j(s_{k+1})\left[\sum_{s_{k+1}} \vartheta_j(s_{k+1})\right]^{-1} \text{ ,}$$

$$\vartheta_j(s_{k+1}) = \tilde{p}_j(s_{k+1})\left[\Theta_j(s_{k+1})\right]^{-1/2} \exp(-h_j(s_{k+1})) \text{ ,}$$

$$\Theta_j(s_{k+1}) = \tilde{R}_j(s_{k+1}) + Q(s_{k+1}) \text{ ,} \qquad \text{, (3)}$$

$$h_j(s_{k+1}) = 0.5\left[Z_j - \tilde{X}_j(s_{k+1})\right]^2\left[\Theta_j(s_{k+1})\right]^{-1} \text{ ,}$$

$$\tilde{p}_j(s_k) = p_j(s_k) \text{ , } s_{k+1} = 1...n \text{ , } j = 1...m \text{ ,}$$

где $Q(s_k)$ - дисперсия ошибки измерений параметра χ;

Z_k - измеренное значение χ ;

s_k - состояния структуры ;

$p(s_k)$ - вероятность состояния структуры системы;

$\tilde{X}(s_k), \tilde{R}(s_k)$ - математическое ожидание и дисперсия параметра χ для состояния s_k ;

m - количество обнаруженных субъектов для идентификации;

n - количество состояний структуры.

Принятие решения о принадлежности субъекта к классу A_1 будет выполняться по уравнению:

h-й субъект относится к классу A_1, если

$$p_h(1) \geq p_{por} \text{ , } p_h(1) = \max_j\{p_j(1)\}, \quad j = 1...m \text{ ,} \qquad (4)$$

где *h* - номер возможного субъекта класса A_1 ;

p(1)- вероятность принадлежности *j* субъекта к классу A_1 ;

p_{por} - пороговое значение вероятности принятия решения.

Скорость сходимости полученной оценки вероятности зависит от дисперсии измерений (априорно назначаемой в зависимости от соотношения сигнал-шум), измеряемой величины и соответствия априорных законов распределения для идентифицируемых субъектов. Определение априорных показателей можно выполнить на основе параметрической аппроксимации от первых двух условных моментов, изложенной в [3].

В качестве примера на рис.1 приведены реализации процессов оценки вероятности идентификации субъекта в зависимости от номера измерений при двух состояниях системы (1 – идентифицируемый субъект класса A1, 2 - субъект класса A2). Необходимо идентифицировать принадлежность наблюдаемого субъекта к одному из заданных классов. Условия реализации примера: $\tilde{X}(1)$ = 1.4 ед., $\tilde{X}(2)$ = 2 ед., $\tilde{R}(1)$ = 0.25 ед., $\tilde{R}$ (2) = 0.04 ед., Q = 0,01ед. Математические ожидания измерений, подаваемых на идентификатор были приняты Z = 1.3; 1.6; 1.9; 2.2; 2.5.

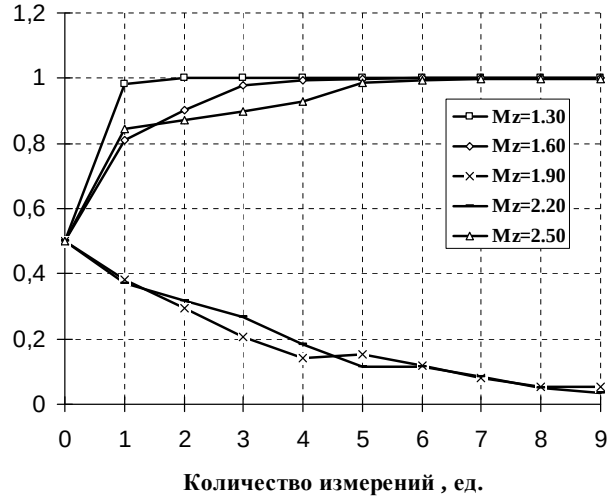

Рис.1. Оценка вероятности идентификации субъекта в зависимости от номера измерений

Оценка вероятности в рассматриваемом алгоритме сходится к значениям вероятности 1 (субъект класса A1) или 0 (субъект класса A2). Скорость сходимости тем больше, чем более выражены отличия параметров идентифицируемых субъектов. На рис.2 приведены законы распределения числа измерений, потребных для идентификации субъектов классификатором в случае, если наблюдается искомый субъект: Z= 1.6, $\tilde{X}(1)$= 1.5; $\tilde{X}(2)$=1.8; $\tilde{R}$ (1) = 0.04; $\tilde{R}$ (2) = 0.25 ; Q = 0.05; 0.15; 0.25.

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.

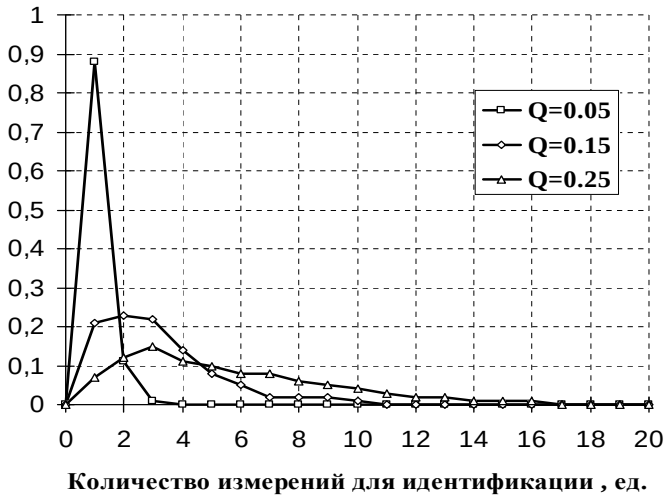

Рис.2. Закон распределения числа измерений, необходимых для идентификации субъекта

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.