А.В Яковлев., А.А. Тихомирова, А.Н. Мазалов

ПОСТРОЕНИЕ ДИНАМИЧЕСКОЙ СЕТЕВОЙ МОДЕЛИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ПО БЕСПРОВОДНОМУ КАНАЛУ

Россия, г. Тамбов, Тамбовский государственный технический университет

The possibility of using a smartphone with the installed specialized software as an identifier for the access control systems, as well as the use of Bluetooth wireless data transfer technology as a wireless channel for transmitting the identifier to the reader of this system, are described. A formal description of the wireless access control system is given. The process of opening the locking device in our wireless access control system using a Petri net apparatus is simulated. The properties of the designed dynamic network model are analyzed.

Сегодня все больше организаций и компаний считают обеспечение безопасности, в частности, организацию пропускного режима с помощью систем контроля и управления доступом (СКУД), одним из важнейших направлений в своей деятельности. Существующие системы, например, на основе *RFID*-карт, смарт-карт и магнитных карт, требуют затрат на выпуск индивидуальных идентификаторов, а также приносят неудобства пользователю, которому необходимо хранить множество различных идентификаторов. Другие же системы, например, на основе биометрических признаков человека, обладают высокой стоимостью, а некоторые из них неработоспособны в агрессивной среде.

Решить эти проблемы может решить система контроля и управления доступом на основе смартфонов с установленным специальным программным обеспечением, в состав которой входит программно-аппаратный комплекс управления преграждающими устройствами по беспроводному каналу.

Целью данной работы является построение динамической сетевой модели функционирования преграждающего устройства системы контроля и управления доступом по беспроводному каналу.

Системы контроля и управления доступом такого типа основаны на передаче идентификатора пользователя на считыватель по беспроводному каналу. Идентификатором может быть: некоторый код, пара логин-пароль, специальный маркер. В качестве беспроводного канала в проектируемой СКУД будет использоваться технология беспроводной передачи данных *Bluetooth*, которая обладает рядом достоинств по сравнению с другими современными технологиями (например, *Wi-Fi, NFC* (*Near Field Communication*), мобильный интернет), таких как:

– возможность передачи данных между устройствами на расстоянии до 100 метров [1];

– малый размер современных модулей, поддерживающих протокол с низким энергопотреблением и встроенным шифрованием (*AES*) [2];

– широкое распространение (в 2018 году 100 % проданных смартфонов и планшетов поддерживают *Bluetooth* [3]).

К преимуществам системы на основе смартфонов с установленным специальным программным обеспечением можно отнести:

– отсутствие необходимости в выпуске индивидуальных устройств идентификации, например, таких как *RFID*-карты (следовательно, отсутствие затрат на их выпуск);

– простота выдачи временных пропусков;

– возможность использования биометрических систем, встроенных в некоторые современные смартфоны, для двухфакторной идентификации;

– возможность использования нескольких аккаунтов одним человеком.

Данные преимущества позволяют использовать смартфон в качестве идентификатора и дают возможность начать проектировать систему на основе беспроводного канала *Bluetooth*.

Рассмотрим алгоритм взаимодействия между компонентами разрабатываемой СКУД.

Доступ в СКУД основан на проверке маркера доступа, выдаваемого субъекту сервером аутентификации на основе его логина и пароля. Маркер содержит разрешения субъекта и его идентификационный номер. Контроллер сравнивает разрешения субъекта из маркера с требуемыми и выносит решение о доступе к объекту. Передача и получение маркера, логина и пароля реализуется по беспроводному каналу передачи данных (*Bluetooth)* между смартфоном субъекта и контроллером. Схема разрабатываемой СКУД приведена на рисунке 1.

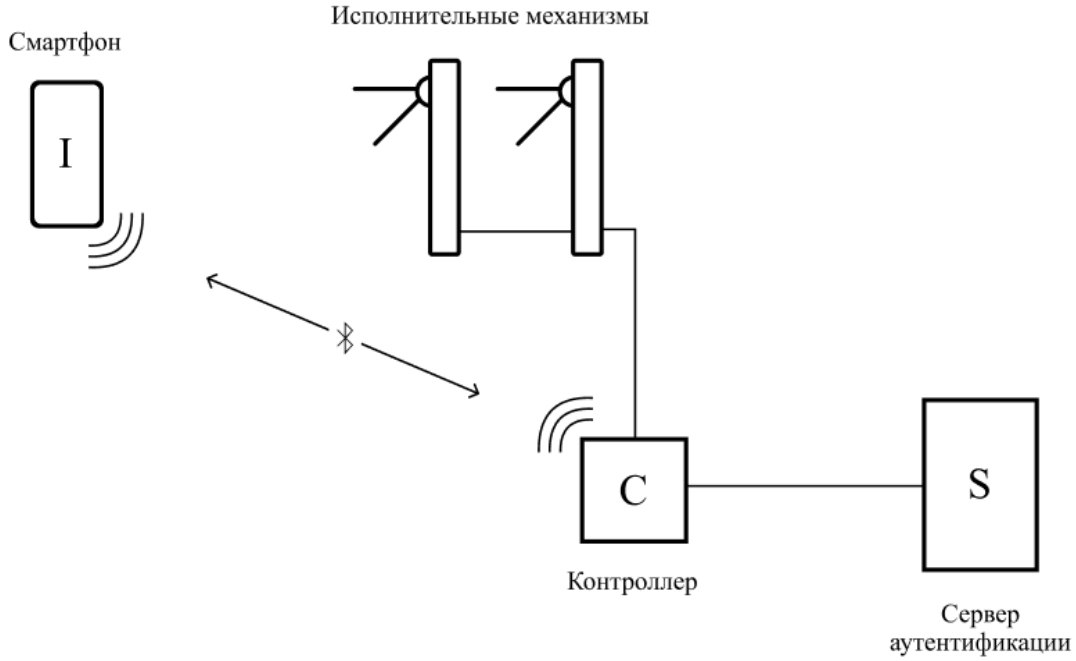

Рисунок 1 – Схема разрабатываемой системы контроля и управления доступом

Маркер доступа выполнен по стандарту *JSON Web Token*. Данный стандарт описывает маркеры доступа на основе формата *JSON*. Маркер состоит из трех частей: заголовок, полезная нагрузка и подпись [4].

Маркер создаётся сервером аутентификации, подписывается секретным ключом и отправляется на смартфон субъекта, который далее использует данный маркер для подтверждения своей личности.

В качестве хранилища данных о субъекта на сервере аутентификации используется реляционная база данных. Её можно описать с помощью *ER*-диаграммы в нотации Гордона Эвереста [5]. Данная диаграмма показана на рисунке 2.

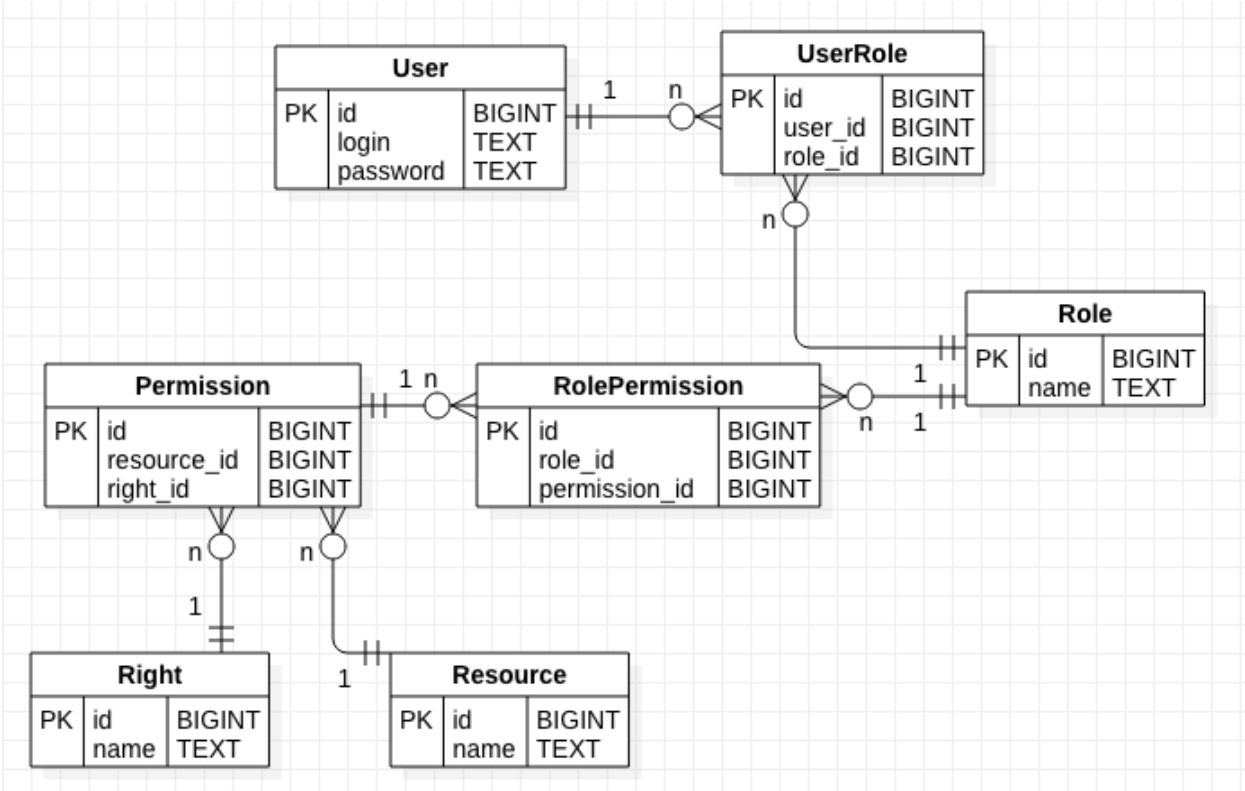

Рисунок 2 – *ER*-диаграмма базы данных

Осуществлять редактирование, создание и удаление пользователей можно с помощью панели администрирования, встроенной в сервер аутентификации.

Для того чтобы впоследствии перейти к программно-аппаратной реализации прототипа (пилотного проекта) описанной системы, построим модель управления ее функционированием на основе сети Петри.

Модель, реализуемая на сети Петри, определяется как пятёрка $<P, T, I, O, \mu>$, где P и T – конечные множества позиций и переходов, I и O – множества входных и выходных функций, μ – множество маркировок состояний [6]. Входная функция I отображает переход t_j в множество позиций $I(t_j)$, а выходная функция O отображает переход t_j в множество позиций $O(t_j)$ [7].

Выполнение сети Петри осуществляется посредством запусков переходов. Переход запускается удалением меток из его входных позиций и образованием новых меток, помещаемых в его выходные позиции. Переход может запускаться только в том случае, когда он разрешён, т.е. если каждая из его входных позиций имеет число меток, по крайней мере, равное числу дуг из позиций в переход.

Событийность при моделировании на сетях Петри определяется действиями происходящими в системе, а также состояниями предшествующими запускам переходов и состояниями после выполнения действий. Анализ результатов выполнения сети может сказать о том, в каких состояниях пребывала или не пребывала система, какие состояния не достижимы.

Проведем моделирование процесса открытия преграждающего устройства в разрабатываемой системе контроля и управления доступом по беспроводному каналу на основе полученной модели. Обозначение элементов этой модели следующие:

– конечное множество позиций:

$P = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}\}$.

– конечное множество переходов:

$T = \{t_0, t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9, t_{10}, t_{11}, t_{12}, t_{13}, t_{14}, t_{15}\}$.

– множество входных позиций перехода:

$I=\{I(t_0), I(t_1), I(t_2), I(t_3), I(t_4), I(t_5), I(t_6), I(t_7), I(t_8), I(t_9), I(t_{10}), I(t_{11}), I(t_{12}), I(t_{13}), I(t_{14}), I(t_{15})\}$.

$I(t_0)=\{p_0\}$, $I(t_1)=\{p_2\}$, $I(t_2)=\{p_3\}$, $I(t_3)=\{p_4\}$, $I(t_4)=\{p_5\}$, $I(t_5)=\{p_6\}$, $I(t_6)=\{p_7\}$, $I(t_7)=\{p_8\}$, $I(t_8)=\{p_1\}$, $I(t_9)=\{p_9\}$, $I(t_{10})=\{p_{10}\}$, $I(t_{11})=\{p_{11}\}$, $I(t_{12})=\{p_{12}\}$, $I(t_{13})=\{p_{13}\}$, $I(t_{14})=\{p_{14}\}$, $I(t_{15})=\{p_{15}\}$.

– множество выходных позиций перехода:

$O = \{O(t_0), O(t_1), O(t_2), O(t_3), O(t_4), O(t_5), O(t_6), O(t_7), O(t_8), O(t_9), O(t_{10}), O(t_{11}), O(t_{12}), O(t_{13}), O(t_{14}), O(t_{15})\}$.

$O(t_0)=\{p_2\}$, $O(t_1)=\{p_3\}$, $O(t_2)=\{p_4, p_6\}$, $O(t_3)=\{p_5\}$, $O(t_4)=\{p_0\}$, $O(t_5)=\{p_7\}$, $O(t_6)=\{p_8\}$, $O(t_7)=\{p_1\}$, $O(t_8)=\{p_9\}$, $O(t_9)=\{p_{10}, p_{14}, p_{15}\}$, $O(t_{10})=\{p_{11}, p_{13}\}$, $O(t_{11})=\{p_{12}\}$, $O(t_{12})=\{p_1\}$, $O(t_{13})=\{p_1\}$, $O(t_{14})=\{p_1\}$, $O(t_{15})=\{p_1\}$.

– начальная маркировка:

$\mu_0 = \{1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\}$.

Описание позиций сети Петри, моделирующей процесс открытия преграждающего устройства в разрабатываемой системе, представлено в таблице 1.

Таблица 1 – Описание позиций сети Петри, моделирующей процесс открытия преграждающего устройства в разрабатываемой системе

Позиция модели	Описание позиции
p_0	Субъект без маркера доступа
p_1	Субъект с маркером доступа
p_2	Контроллер получил логин и пароль субъекта
p_3	Сервер получил логин и пароль субъекта
p_4	Сервер не обнаружил совпадений в БД субъектов
p_5	Контроллер получил сообщение об ошибке
p_6	Сервер обнаружил субъекта в БД
p_7	Сервер сгенерировал маркер доступа субъекта
p_8	Контроллер получил маркер доступа от сервера
p_9	Контроллер получил маркер доступа от субъекта
p_{10}	Маркер успешно верифицирован контроллером
p_{11}	Маркер содержит необходимые разрешения
p_{12}	Преграждающее устройство открыто
p_{13}	Маркер не содержит необходимых разрешений
p_{14}	Маркер с истекшем сроком действия
p_{15}	Маркер с невалидной подписью

Содержание переходов сети Петри, моделирующей процесс открытия преграждающего устройства в разрабатываемой системе, представлено в таблице 2.

Таблица 2 – Содержание переходов сети Петри, моделирующей процесс открытия преграждающего устройства в разрабатываемой системе

Переход модели	Описание перехода
t_0	Передача логина и пароля на контроллер
t_1	Передача логина и пароля на сервер
t_2	Поиск субъекта в БД
t_3	Передача сообщения об ошибке на контроллер
t_4	Передача сообщения об ошибке субъекту
t_5	Генерация маркера доступа субъекта

Переход модели	Описание перехода
t_6	Передача маркера доступа с сервера на контроллер
t_7	Передача маркера доступа субъекту
t_8	Передача маркера доступа от субъекта на контроллер
t_9	Верификация маркера доступа
t_{10}	Проверка разрешений маркера доступа
t_{11}	Открытие преграждающего устройства
t_{12}	Передача сообщения об успешном открытии объекта
t_{13}, t_{14}, t_{15}	Передача сообщения об ошибке субъекту

Сеть Петри, моделирующая процесс открытия преграждающего устройства в разрабатываемой системе, изображена на рисунке 3.

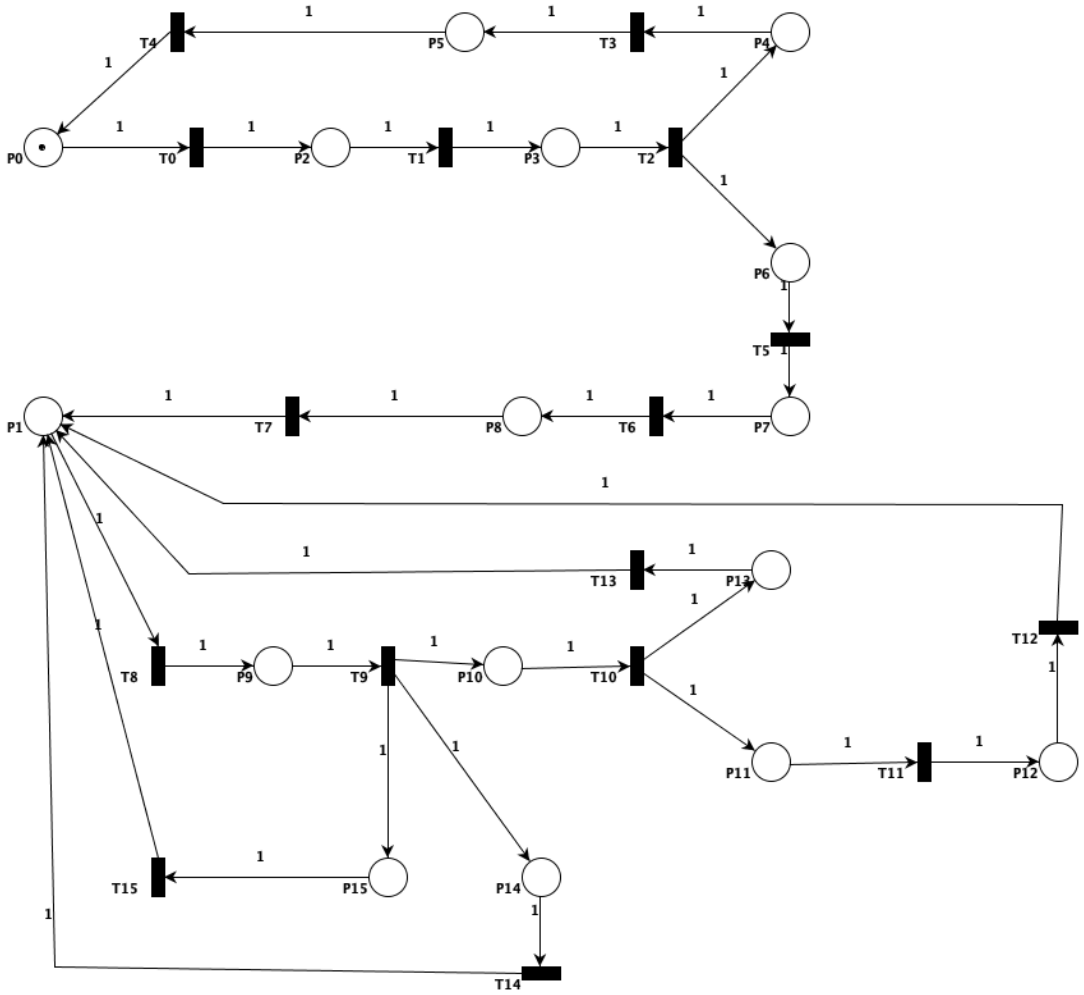

Рисунок 3 – Сеть Петри, моделирующая процесс открытия преграждающего устройства в разрабатываемой системе

Проведём анализ полученной модели на базе основных свойств сетей Петри: безопасности, ограниченности, устойчивости, достижимости и активности. Введём определение каждого из этих свойств и, исходя из них, дадим характеристику построенной модели.

Позиция $p_i \in P$ называется безопасной в заданной начальной маркировке μ, если в

процессе работы этой сети в данной позиции p_i никогда не появится более одной фишки (маркера), то есть $\mu(p_i) \leq 1$. Сеть Петри называется безопасной, если безопасны все ее позиции [8].

Из данного определения следует, что модель, представленная сетью Петри, реализующая процесс открытия преграждающего устройства в разрабатываемой системе, является безопасной, так как в позициях данной сети не происходит накопление фишек.

Позиция $p_i \in P$ называется ограниченной в заданной начальной маркировке μ, если в процессе работы этой сети в данной позиции p_i никогда не появится более k маркеров, то есть $\mu(p_i) \leq k$. Сеть Петри называется ограниченной, если ограничены все ее позиции [8].

Модель, имитирующая процесс открытия преграждающего устройства в разрабатываемой системе, является ограниченной со значением $k = 1$, так как число меток в каждой позиции никогда не превысит значения $k = 1$.

Сеть Петри называется устойчивой, если для любого ее перехода $t_i \in T$ выполняется следующее условие: состояние возбуждения этого перехода не может быть снято срабатыванием другого какого-либо перехода. Если в сети имеются альтернативные переходы, то она является неустойчивой [8].

В сети, процесс открытия преграждающего устройства в СКУД, имеются альтернативные переходы, например переходы t_2, t_9, t_{10}, следовательно, данная сеть является неустойчивой.

Маркировка μ' называется достижимой из некоторой маркировки μ, если для данной модели сети Петри можно указать такую последовательность срабатывания переходов, которая переводит маркировку μ в маркировку μ' [8].

Отсутствие тупиковых переходов в модели, представленной на рисунке 3, позволяет утверждать о достижимости ее маркировок.

Переход $t_i \in T$ называется активным в заданной начальной маркировке μ, если для любой маркировки μ', достижимой из μ, можно указать цепочку срабатывания переходов, которая привод к возбуждению перехода t_i. Сеть называется активной в заданной начальной маркировке μ, если активны все её переходы [8].

Сеть Петри, моделирующая процесс открытия преграждающего устройства в разрабатываемой системе, является активной, так как все её переходы активны, а состояния достижимы при начальной маркировке μ и можно определить последовательность срабатывания переходов, которая приведёт в то или иное состояние.

Построенная динамическая сетевая модель системы контроля и управления доступом по беспроводному каналу имеет строгое формальное описание, позволяющее провести анализ процесса взаимодействия трех субъектов информационных отношений, а именно пользователя, контроллера и сервера аутентификации. Данная модель дает возможность перейти к программно-аппаратной реализации прототипа системы контроля и управления доступом по беспроводному каналу.

1. Что такое Bluetooth и как он работает. [Электронный ресурс]: Режим доступа: http://1234g.ru/blog-of-wireless-technologies/bluetooth/chto-takoe-bluetooth-i-kak-on-rabotaet

2. Bluetooth Security 101. [Электронный ресурс]: Режим доступа: https://www.bluetooth.com/blog/bluetooth-security-101/

3. The IoT for Everyone. [Электронный ресурс]: Режим доступа: https://www.bluetooth.com/markets/phone-pc/

4. Пять простых шагов для понимания JSON Web Tokens. [Электронный ресурс]:

Режим доступа: https://habr.com/post/340146/

5. Концептуальная модель базы данных: Нотация Гордона Эверста. [Электронный ресурс]: Режим доступа: https://webonto.ru/kontseptualnaya-model-bazyi-dannyih/#_Gordon_Everest

6. Котов, В.Е. Сети Петри / В.Е. Котов – М.: Наука, 1984. – 160 с.

7. Питерсон, Дж. Теория сетей Петри и моделирование систем / Дж. Питерсон. – М.: Мир, 1984. – 264 с.

8. Радько, Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н.М. Радько, И.О. Скобелев. – М.: РадиоСофт, 2010. – 232 с.