# АЛГОРИТМ И РЕАЛИЗАЦИЯ ИНТЕЛЛЕКТУАЛЬНОГО ВЫБОРА МОДЕЛИ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В ИНФОКОММУНИКАЦИЯХ

В.А. ВИШНЯКОВ[1], М.М. ГОНДАГ САЗ[2]

*Учреждение образования «Белорусская государственная академия связи», ул. Ф. Скорины, 8/2, Минск, 220114, Беларусь*

*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ул. П. Бровки, 6, Минск, 220013, Беларусь*

*Поступила в редакцию 18 ноября 2019*

Предложен интеллектуальный алгоритм выбора конкретного метода аутентификации для пользователей мобильных приложений, основанный на технологии экспертных систем. Разработана и реализована программная структура такой системы и приведены расчеты ее стоимости и эффективности.

*Ключевые слова:* модели аутентификации, интеллектуальный алгоритм, интеллектуальная система, эффективность.

## Введение

Надежный доступ к инфокоммуникационным ресурсам один из ключевых компонентов информационной безопасности. Управление доступом, передача информации, межсетевые экраны, виртуальные частные сети базируются на аутентификации и выдаче прав доступа к ресурсам, с которыми устанавливается соединение [1]. Известно большое количество видов аутентификации, но часто используется многоразовый пароль (МП) [1, 2]. Однако этот вид аутентификации не совсем надежен и в отдельных случаях плохо влияет на обеспечение информационной защиты локальных сетей и мобильных приложений. Для предотвращения возможности нарушения конфиденциальности, доступности и целостности в мобильных приложениях следует выполнять рекомендации по частому изменению МП и использовать варианты строгой аутентификации [1]. Но это требует больших вычислительных ресурсов, относительно дорого. Для администратора хорошо бы иметь интеллектуального помощника по выбору вида аутентификации в зависимости от ситуации и ряда факторов [3]. Поэтому в статье представлен алгоритм и реализация интеллектуального выбора вида доступа к мобильным приложениям с оценкой его экономической эффективности.

## Интеллектуальный алгоритм выбора модели аутентификации

Для выбора того или другого вида (модели) аутентификации [4] нужно понимать как различия технологий при их использовании, так и затраты на реализацию, что требует применения интеллектуальных технологий. Интеллектуальный подход к выбору той или иной модели доступа пользователя базируется на технологии экспертных систем [5]. Подход заключается в создании интеллектуальной системы аутентификации (ИСА), которая будет включать базы данных и знаний, решатель и интерфейс эксперта и пользователя. Рассмотрим построение ИСА на структурно-алгоритмическом уровне, ее программную реализацию и оценку эффективности. Определим структуру ИСА, включающую базу данных (БД) и знаний, интерфейс эксперта и администратора, интеллектуальный решатель [5–6].

В БЗ будут храниться модели аутентификации, критерии их выбора, вопросы к администратору (пользователю) для оценки ситуации безопасности, правила оценки моделей аутентификации по критериям, правила выбора модели по ответам администратора. Решатель по содержимому БЗ будет вычислять подходящий вид (модель аутентификации). Через интерфейс эксперта формируется БЗ ИСА, а через интерфейс пользователя вводятся вопросы

к администратору и его ответы по оценке ситуации информационной безопасности (ИБ) для пользователей, для которых и определяется тот или иной вид доступа. Представим информацию, необходимую для БЗ ИСА.

Определим факторы, по которым будет вычисляться общая оценка модели аутентификации:

$$F = \{f_1, \dots f_k\},$$

где $f_1$ − разновидность ввода кода; $f_2$ − тип считывающего устройства; $f_3$ − стойкость; $f_4$ − затраты на разработку и внедрение; $f_5$ − трудность использования для клиента; $f_6$ − применимость удаленного доступа; $f_7$ − множественность настроек; $f_8$ − степень стойкости от настроек; $f_9$ − распространение в использовании; $f_{10}$ − срок хранения аутентифицирующей информации; $f_{11}$ − вероятность ошибок; $f_{12}$ − наличие нормативной документации.

Выбрав ряд факторов, можно провести сравнительную оценку различных технологий аутентификации при том или ином решении. На базе факторов, перечисленных выше, будет происходить выбор модели (оценка) различных разновидностей аутентификации:

$$A = \{a_1, \dots a_5\},$$

где $a_1$ − аутентификация с использованием многоразового пароля (МП); $a_2$ – аутентификация с использованием одноразового пароля (ОП); $a_3$ – аутентификация по персональному токену (Т); $a_1$ − двухфакторная аутентификация (2ФА); $a_1$ − биометрическая аутентификация (БА).

Определим правила соответствия факторов и моделей аутентификации (табл. 1).

Таблица 1. Соответствие факторов и моделей аутентификации

| Модель аутентификации / Факторы | МП | ОП | Т | 2ФА | БА |
|---|---|---|---|---|---|
| 1 Метод ввода | клавишный | клавишный | доп | доп | б |
| 2 Доп. устр. ввода | | | + | + | + |
| 3 Стойкость | низ | выс | сред | выс | выс |
| 4 Затраты | низ | сред | сред | выс | выс |
| 5 Сложность эксплуатации | низ | сред | сред | выс | низ |
| 6 Удаленная аутентификация | + | + | - | + | - |
| 7 Настройки | сред | выс | низ | выс | сред |
| 8 Стоимость настроек | сред | выс | сред | выс | сред |
| 9 Распространение | выс | выс | сред | сред | низ |
| 10 Срок хранения | низ | выс | сред | выс | выс |
| 11 Вероятность ошибки | выс | сред | сред | низ | низ |
| 12 Наличие документации | сред | сред | низ | сред | низ |

Для оценки ситуации по ИБ администратор отвечает на ряд вопросов с двумя вариантами ответа «ДА/НЕТ»:

$$V = \{v_1, \dots v_N\},$$

где $v_1$ − возможно ли подключение дополнительных устройств (ДУ)?; $v_2$ − наличие пользователей с ограниченными возможностями (ПОВ)?; $v_3$ − возможна ли выдача токена (Т)?; $v_4$ − возможна ли двухфакторная аутентификация (2ФА)?; $v_5$ − постоянно ли число пользователей (ПЧП)?; $v_6$ − наличие пользователей с низкой компетенцией (ПНК)?; $v_7$ − локальная аутентификация (ЛА)?; $v_8$ − высокие затраты на внедрение и обслуживание (ВЗВ)?; $v_9$ − степень ценности защищаемой информации (СЦИ)?; $v_{10}$ − необходимость удаленной аутентификации (УА); $v_{11}$ − клавиатурный вид ввода (КВ); $v_{12}$ − ввод через дополнительные сенсоры (ДСВ).

Далее определяем правила соответствия положительных ответов на вопросы множества $V$ и моделей аутентификации $R = O \cdot A$:

Если $v_1$, то Т или БА;
Если $v_2$, то Т или БА;
Если $v_3$, то Т;
Если $v_4$, то 2ФА;
Если $v_5$, то МП;
Если $v_6$, то Т или БА;
Если $v_7$, То МП или Т;
Если $v_8$, то 2ФА или БА;
Если $v_9$, то ОП или 2ФА;
Если $v_{10}$, то ОП или 2ФА;
Если $v_{11}$, то МП или ОП;
Если $v_{12}$, то Т или БА.

Данные положения были положены в основу алгоритма по интеллектуальному выбору вида доступа пользователей к мобильным приложениям.

Для параметрического интеллектуального выбора наиболее подходящего вида аутентификации интеллектуальный алгоритм, положенный в основу экспертной системы (ЭС) включает шаги:

1. Наполнение базы знаний ИСА инженером по знаниям.

1.1 Формирование и ввод видов (моделей) аутентификации $A = \{a_1, \dots a_5\}$, где $a_1, \dots a_M$ – модели аутентификации (пять моделей).

1.2 Формирование и ввод факторов аутентификации $F = \{f_1, \dots f_k\}$, где $f_1, \dots f_k$ – варианты критериев выбора того или иного вида.

1.3 Формирование и ввод правил соответствия моделей аутентификации и факторов $S = A \cdot F$.

1.4 Формулирование и ввод вопросов для оценки ситуации ИБ $V = \{v_1, \dots v_N\}$, где $v_1, \dots v_N$ – все вопросы администратору (пользователю).

1.5 Формулирование и ввод правил соответствия ответов на вопросы и факторов $S = A \cdot F$.

2. Описание ситуации по ИБ и работа ЭС.

2.1 Получение ответов администратора на вопросы $V$: $O = \{o_1, \dots, o_N\}$.

2.2 На основании ответов будут определены элементы множеств критериев и методов аутентификации, будет получена качественная оценка критериев (низкий, средний, высокий), которым поставим в соответствие количественную оценку (0, 1, 2).

2.3 Согласно количественной оценке критериев будет выявлен лучший метод аутентификации (работа решателя).

3. Работа решателя, который вычисляет следующее:

3.1 Строится подмножество выбранных для сравнения факторов $F' \in F$. Данное множество $F'$ строится на основании правил соответствия ответов на вопросы и факторов $M_{ij} = O \cdot F$, где $i$ – вопрос, $j$ – фактор. Если ответ $o_n$ на вопрос $v_i$ утвердительный, то $o_n(v_i) = 1$, учитываем данный $j$-критерий.

3.2 Определяется наилучший метод аутентификации как среднеарифметическое значение таблицы сравнений методов аутентификации по выбранным критериям (табл. 1.). Лучший метод аутентификации $A_{bet}$ определяется как наибольший для каждого метода $A_p$ по формуле:

$$A_{bet} = \max (A_p = 1/w \sum t_{mi}),\ i = 0, \dots, w.$$

где критерии определяются из подмножества $T \in C$, $w$-мощность множества $T$, $p$ – текущий метод аутентификации из множества $A$.

4. Через интерфейс пользователя выводится значение $A_{bet}$.

Программная реализация ИСА

Процесс разработки физической структуры программного продукта ИСА инструментами Visual Studio начинается с формирования пользовательского интерфейса и разработки кода и различных рабочих форм с учетом эргономичности, эстетичности, минимализма. При разработке программы использовано два вида форм:

− формы, которые создаются при запуске программы и затем при открытии или закрытии просто прорисовываются либо скрываются;

− диалоговые окна, уведомляющие пользователя о произошедшем событии. При работе с такими окнами нельзя начать работу с какими-либо другими формами? пока это окно не будет закрыто.

События, использованные на форме FormText:

– private void private void init_teft() – м Visual Studio метод инициализации формы, где объявляются основные переменные;

– private void private void load_vueftionf() – обработчик загрузки вопросов для прохождения опроса;

– private void fhow_vueftion() – обработчик события отображения вопроса и вариантов ответа;

– private void button_next_Click – обработчик события клика по кнопке «далее», где сохраняется ответ пользователя;

– private void show_result() – обработчик события отображения результата.

Структура программного средства ИСА для автоматизации выбора наиболее рационального метода аутентификации состоит из трех основных модулей:

− БЗ (модуль опроса). Отвечает за проведение опроса, вводит запись выбранных пользователем ответов;

− решатель (модуль оценки). Проводит анализ полученных данных в виде ответов, оценивает и подбирает наиболее подходящий метод аутентификации;

− пользовательский интерфейс. Отображает подобранный метод аутентификации.

При запуске программы пользователю показывается страница с вопросом и двумя вариантами ответа, при ответе на который выбирается лучшая форма аутентификации.

Рассмотрим особенности программной реализации. Системный класс Program содержит в себе единственный статический метод Main, который устанавливает параметры запуска приложения и открывает главное меню программы.

Проект содержит все исходные материалы для приложения (файлы исходного кода), файлы ресурсов (изображения, ссылки на внешние файлы, которые использует программа) и данные конфигурации, такие как параметры компилятора. При построении проекта Visual C# вызывает компилятор C# и другие внутренние средства для создания исполняемой сборки из файлов проекта.

Физическая структура программного средства состоит из следующих файлов: Properties; References; Resources; FormText.cf.

Под узлом «Properties» представлены параметры конфигурации, применяемые ко всему проекту и хранящиеся в файле CFPROJ в папке решения. В контексте проекта узел «References» определяет двоичный файл, необходимый для выполнения приложения. Узел «Resources» представляет собой данные, которые включаются в приложение, но могут храниться таким образом, что их можно будет изменять независимо от остального исходного кода.

С каждой формой связаны два файла. В файле Form1.cf находится исходный код для настройки формы и ее элементов управления, а также их реакции на события. В файле designer.cf содержится исходный код, который записывает Конструктор форм при перетаскивании элементов управления в форму, установке свойств в окне Свойства и так далее.

В файле FormText.cf содержится исходный код опроса пользователя и вычисление результата, на основе которого определяется метод аутентификации.

Процесс разработки физической структуры разрабатываемого программного продукта инструментами Visual Studio начинается с формирования пользовательского интерфейса и разработки кода и различных рабочих форм с учетом эргономичности, эстетичности, минимализма. При разработке программы использовано два вида форм:

− формы, которые создаются при запуске программы, и затем при открытии или закрытии просто прорисовываются либо скрываются;

− диалоговые окна, уведомляющие пользователя о произошедшем событии. При работе с такими окнами нельзя начать работу с какими-либо другими формами пока это окно не будет закрыто.

События, использованные на форме FormText:

– private void private void init_teft() – метод инициализации базы знаний (БЗ), где объявляются основные переменные;

– private void private void load_vueftionf() – обработчик загрузки вопросов в БЗ для прохождения опроса;

– private void fhow_vueftion() – обработчик решателя отображения вопроса и вариантов ответа;

– private void button_next_Click – обработчик решателя по кнопке далее, где сохраняется ответ пользователя;

– private void fhow_refult()– обработчик события отображения результата.

При запуске программы ИСА пользователю показывается страница с вопросом и двумя вариантами ответа.

Пользователю необходимо выбрать один из вариантов ответа (Да/Нет) для всех 12 вопросов. При отсутствии варианта ответа вопрос не засчитывается выводом ошибки. После прохождения опроса программа, на основании ответов пользователя, определит наиболее подходящий метод аутентификации и выведет его на экран.

**Определение стоимости ИСА и ее эффективности**

Объем программного средства (ПС) ИСА определяется исходя из количества функций, реализуемых ПС, которые представлены в табл. 2, и рассчитывается как их сумма. Среда разработки программного обеспечения (ПО) – Microsoft Visual Studio.

Таблица 2. Функции, реализуемые программой ИСА

| Номер | Наименование (содержание) функции | Объем функции $V_i$ |
|---|---|---|
| 101 | Организация ввода информации | 50 |
| 102 | Контроль, обработка и ввод информации | 180 |
| 109 | Организация ввода/вывода информации | 70 |
| 111 | Управление вводом/выводом | 940 |
| 405 | Система настройки ПО | 100 |
| 506 | Обработка ошибочных и сбойных ситуаций | 140 |
| 507 | Обеспечение интерфейса между компонентами | 240 |
| 703 | Расчет показателей | 160 |
| 707 | Графический вывод результатов | 105 |
| Итого общий объем ПС | | 1985 |

На основании общего объема ПС определяется нормативная трудоемкость $Т_н$ с учетом сложности ПС. Так как разрабатываемый продукт относится к третьей группе сложности, то нормативная трудоемкость составляет $Т_н = 44$ чел./дней.

На основании общей трудоемкости разработки ПС и установленного периода разработки в один месяц (22 рабочих дня) устанавливается общая плановая численность разработчиков:

$$Ч_р = 44 / 22 = 2 \text{ чел.}$$

Численность разработчиков и трудоемкость служат базой для расчета основной заработной платы. Основная заработная плата разработчиков принимается в 1100 руб/мес (средняя по республике). Коэффициент премирования – 20 %:

$$З_{пр} = 1100 \cdot 2 \cdot 1{,}2 = 2880 \text{ руб.}$$

Отчисления на социальные нужды включают в предусмотренные законодательством отчисления в фонд социальной защиты и фонд обязательного страхования (34,6 %):

$$О_{сн} = 2880 \cdot 0,\ 346 = 996{,}5 \text{ руб.}$$

Норма расхода материалов – 3 % от основной зарплаты.

$$С_м = 2880 \cdot 0{,}03 = 84{,}5 \text{ руб.}$$

Расходы на потребляемую электроэнергию с учетом работы двух разработчиков, 22 дня по 8 часов в день, стоимость 1 кВт/час – 0,18 руб, мощности компьютеров – 0,2 кВт:

$$С_э = 0{,}18 \cdot 0{,}2 \cdot 8 \cdot 22 \cdot 2 = 13 \text{ руб.}$$

Расходы по статье «Прочие затраты» определяются исходя из нормы 5 % от зарплаты:

$$Р_{пз} = 2880 \cdot 0{,}05 = 144 \text{ руб.}$$

Расходы по статье «Накладные расходы» определяются исходя из нормы 5 % от зарплаты:

$$Р_{нр} = 2880 \cdot 0{,}1 = 288 \text{ руб.}$$

Тогда себестоимость программы ИСА составит:

$$С_{иса} = 2880 + 996,5 + 84,5 + 13 + 144 + 288 = 4406 \text{ руб.}$$

Сметой предусматриваются не только затраты (основная зарплата, премия, начисления на зарплату и т. д.), но и налоги, предусмотренные законодательством, и прибыль организации-разработчика 10 %.

$$П_р = 4406 \cdot 0,1 = 440,6 \text{ руб.}$$

Отпускная цена Циса программы ИСА включает в себя себестоимость, прибыль, налог на добавленную стоимость (20 %) и налог на прибыль (18 %):

$$НДС = 4406 \cdot 20 / 120 = 744,3 \text{ руб,}$$

$$Н_{пр} = 440,6 \cdot 18 / 100 = 79,3 \text{ руб,}$$

$$Ц_{иса} = 4406 + 440,6 + 744,3 + 79,3 = 5670,2 \text{ руб.}$$

В результате расчетов цена готового продукта составляет 5670,2 руб.

Курс Национального банка Республики Беларусь на момент расчета 1 долл. – 2,05 руб. Тогда цена программы в долларах:

$$Ц_{исад} = 5670,2 / 2,05 = 2766 \text{ долл.}$$

По данным источника цена аналогичного продукта за рубежом около 6 тыс. долл. [7]. Таким образом, данное программное средство в 2,16 раза дешевле, что подтверждает его эффективность.

## Заключение

1. Разработан интеллектуальный алгоритм для поддержки принятия решения по выбору видов аутентификации пользователей мобильных приложений в конкретной ситуации, которые позволяют по ряду факторов выбрать лучший вариант. Для реализации данных моделей предложен экспертный подход.

2. Разработана структура интеллектуальной системы для выбора модели аутентификации, включающая интерфейс, БЗ, решатель. Администратор формирует наилучший в данных условиях вариант доступа, отвечая на ряд вопросов. Приведены детали программной реализации ИСА с использованием инструментариев системы Visual Studio. Рассчитана цена и эффективность данного средства.

## ALGORITHM AND IMPLEMENTATION OF INTELLIGENT CHOICE OF ACCESS MODEL FOR MOBILE APPLICATIONS USERS IN INFOCOMMUNICATIONS

U.A. VISHNIAKOU, M.M. GHONDAGH SAS

An intelligent algorithm for selecting a specific authentication method for mobile application users based on expert systems technology is proposed. The program structure of such system is developed and implemented, and calculations of its cost and efficiency are given.

## Список литературы

1. Смит, Р. И. Аутентификация: от паролей до открытых ключей / Р. И. Смит. – М. : Вильямс, 2002. – 433 с.

2. Бобов, М. Н. Основы аутентификации в телекоммуникационных системах : учеб. пособие / М. Н. Бобов, В. К. Конопелько. – Минск : БГУИР, 2009. – 132 с.

3. Мартынова, Л. Е. Определение критериев оценки для подбора оптимального метода аутентификации / Л. Е Мартынова, К. Е. Назарова, С. М. Попков // Молодой ученый. – 2016. – № 27. – С. 119–122.

4. Выростков, Д. Обзор способов и протоколов аутентификации в веб-приложениях [Электронный ресурс]. – Режим доступа : httpf://habrahabr.ru/company/dataart/blog/262817/. Дата доступа : 12.10.2019.

5. Вишняков, В. А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях : методы, модели, программно-аппаратные решения. Монография / В. А. Вишняков. – Минск : Бестпринт, 2016. – 276 с.

6. Вишняков, В. А. Интеллектуальный выбор вида аутентификации пользователей мобильных приложений / В. А. Вишняков, М. М. Гондаг Саз // Современные средства связи : материалы 24-й

международ. науч. конф., Минск, 17 окт. 2019 г. / Белорус. гос. акад. связи ; редкол.: А. О. Зеневич [и др.]. – Минск, 2019. – С. 158.

7. Современные технологии обеспечения информационной безопасности [Электронный ресурс]. – Режим доступа : http://ipb.mof.ru/ttb l. – Дата доступа : 09.11.2019.