УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 621.391

БУЙ
Павел Михайлович

МЕТОД И СРЕДСТВА ОЦЕНКИ ЭФФЕКТИВНОСТИ УСТРОЙСТВ АУТЕНТИФИКАЦИИ В СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ

Автореферат диссертации на соискание ученой степени
кандидата технических наук
по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Минск, 2008

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель	**Бобов Михаил Никитич**, доктор технических наук, профессор, научно-исследовательское учреждение «НИИ средств автоматизации», заведующий лабораторией
Официальные оппоненты:	**Кучинский Петр Васильевич**, доктор физико-математических наук, научно-исследовательское учреждение «НИИ прикладных физических проблем им А.Н. Савченко при Белорусском государственном университете», заместитель директора
	Иванченко Юрий Иванович, кандидат технических наук, унитарное предприятие «Научно-технический центр «Атлас»», ведущий специалист
Оппонирующая организация	Государственное учреждение «НИИ Вооруженных Сил Республики Беларусь»

Защита состоится 26 июня 2008 года в 16:00 на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники», по адресу 220013, г. Минск, ул. П. Бровки, 6, ауд. 232, 1-й корпус, e-mail: dissovet@bsuir.by, тел.: 293-89-89.

КРАТКОЕ ВВЕДЕНИЕ

Существующие системы защиты информации, прежде чем предоставить субъекту доступ к той или иной информации, должны получить положительные результаты идентификации и аутентификации данного субъекта, для чего предназначены устройства (средства) аутентификации.

Устройство (средство) аутентификации – это программный модуль или аппаратно-программное устройство, которое обеспечивает идентификацию субъекта и устанавливает, является ли он тем, за кого себя выдает.

В литературе по защите информации достаточно широко представлены описания средств и методов аутентификации, однако вопросы формальной оценки их эффективности, учитывающих как конструктивные особенности, так и среду функционирования данных средств, практически не освещены.

Таким образом, возникают задачи в разработке метода оценки эффективности средств аутентификации и требований по их проектированию.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема данной диссертации связана с выполнением двух проектов в рамках Государственной программы информатизации Республики Беларусь на 2003 – 2005 годы и на перспективу до 2010 года «Электронная Беларусь», утвержденной Постановлением СМ РБ от 27.12.2002 г. №1819:

1. Создать единую информационную систему контроля за выполнением поручений Президента Республики Беларусь (ЕИС КВП ПРБ) (Проект №25).

2. Разработать и внедрить первую очередь интегрированной Системы совета по координации контрольной деятельности в Республике Беларусь (проект №41).

Цель и задачи исследования

Целью работы является комплексное исследование и разработка метода оценки средств аутентификации, направленные на повышение эффективности их работы в сетях телекоммуникаций.

Для достижения этой цели необходимо решить следующие задачи:

1. Разработать функциональную структуру и определить обобщенный алгоритм работы средств аутентификации.

2. Выбрать и обосновать показатели эффективности средств аутентификации.

3. Определить методы формальной оценки для требуемых показателей эффективности биометрических средств аутентификации.

4. Синтезировать модель средств аутентификации и провести исследования показателей их эффективности для различных классов опознания.

5. Разработать метод оценки эффективности средств аутентификации и определить требования по их проектированию.

Объектом исследования настоящей работы являются средства аутентификации, используемые в сетях телекоммуникаций. Предметом исследования является эффективность средств аутентификации. Выбор данных объекта и предмета исследования обусловлен актуальностью проблемы создания эффективных средств аутентификации, обеспечивающих требуемый уровень защищенности каналов доступа в сетях телекоммуникаций.

Положения, выносимые на защиту

1. Функциональная структура и обобщенный алгоритм работы средств аутентификации трех классов опознания, основанные на выполнении в определенной последовательности четырех основных функций: обнаружения, опознания, управления и контроля, что позволяет создавать математические модели данных средств, адекватные их реальным функциональным структурам.

2. Аналитические выражения для вычисления вероятности пропуска «чужого» средствами аутентификации по отпечатку пальца и образцу голоса, позволяющие исключить значительные временные затраты на проведение их экспериментальных оценок, и, при заданных параметрах функционирования, определять значения вероятностей пропуска «чужого», которые для исследуемых биометрических средств равны $P_{\text{ОП}} = 0{,}1972 \cdot 10^{-7}$ и $P_{\text{ОГ}} = 0{,}239 \cdot 10^{-7}$ соответственно.

3. Математическая модель средств аутентификации, основанная на описании разрешенных и запрещенных состояний и вероятностных переходов между ними с использованием цепей Маркова, позволяющая определить зависимость эффективности исследуемых средств аутентификации от интенсивности отказов оборудования, согласно которой, при увеличении интенсивности отказов на порядок, эффективность средств аутентификации уменьшается на 15-20%.

4. Метод оценки эффективности средств аутентификации, основанный на использовании обобщенного алгоритма работы средств аутентификации, аналитических выражений для вычисления вероятности правильного опознания субъекта и математической модели средств аутентификации, позволяющий установить степень выполнения требуемых показателей с учетом конкретной реализации средств аутентификации и реальных условий их эксплуатации.

Личный вклад соискателя

В совместных работах участие научного руководителя носит постановочный характер, а лично соискателем выведены аналитические

выражения для получения вероятности подбора биометрического аутентификатора в средствах аутентификации по отпечатку пальца и образцу голоса, синтезирована математическая модель средств аутентификации, осуществлена реализация данной модели и произведена оценка эффективности исследуемых в работе средств аутентификации.

Апробация результатов диссертации

Результаты диссертационной работы докладывались и обсуждались на следующих конференциях: «Технические средства защиты информации»: материалы IV, V Белорусско-российских научно-технических конференций (Нарочь, 2006, 2007 г.); «Актуальные проблемы развития железнодорожного транспорта», научно-практическая конференция посвященная 100-летию профессора И.Г. Тихомирова (Гомель, 2006 г.); «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных»: международный научно-технический семинар (Минск, БГУИР, 2006, 2007 г.).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 8 печатных работ, в том числе: 6 статей в научных журналах общим объемом 2.9 авторских листа; 2 статьи в сборниках и материалах конференций. Без соавторов опубликована 1 статья.

Структура и объем диссертации

Работа состоит из введения, четырех глав, заключения, библиографического списка и приложений. В первой главе представлен обзор современных методов идентификации и аутентификации, методов оценки их эффективности, а также обзор алгоритмов работы наиболее широко используемых на практике средств аутентификации. Во второй главе предложена типовая структура средства аутентификации и построена блок-схема алгоритма его работы, осуществляется выбор показателя эффективности средств аутентификации всех основных классов опознания. Для исследуемых биометрических средств аутентификации, осуществляется вывод аналитических выражений для получения данного показателя эффективности. В третьей главе производится синтез математической модели средств аутентификации и приводится описание реализации данной модели. Четвертая глава содержит описание результатов оценки эффективности исследуемых средств аутентификации с помощью модели, сформулированы требования, которые необходимо предъявлять к эффективным средствам аутентификации при их проектировании, а также представлен разработанный метод оценки эффективности средств аутентификации. Общий объем диссертационной работы составляет 176 страниц, из которых 85 страниц текста, 55 рисунков на

27 страницах, 3 таблицы на 6 страницах, семь приложений на 53 страницах, библиография из 66 источников на 5 страницах, включая 8 собственных публикаций автора на 1 странице.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении дано определение средства аутентификации, обоснована актуальность темы диссертации, показана необходимость разработки метода оценки эффективности средств аутентификации.

В первой главе представлен обзор современных методов идентификации и установления подлинности субъектов, которые, в общем случае, разбиты на три основных класса опознания, базирующихся на [2-А, 7-А]:

а) условных, заранее присваиваемых признаках (сведениях), известных субъекту (что знает субъект);

б) физических средствах, действующих аналогично физическому ключу (что имеет субъект);

в) индивидуальных характеристиках субъекта, его физических данных, позволяющих выделить его среди других лиц (что присуще субъекту).

Здесь же рассмотрены алгоритмы работы наиболее широко используемых на практике средств аутентификации всех классов опознания: средства парольной аутентификации пользователей в операционных системах (ОС) MS Windows XP и UNIX, средства аутентификации с использованием смарт-карт и электронных ключей iButton, средства аутентификации пользователей по отпечатку пальца и образцу голоса.

Обзор алгоритмов работы средств аутентификации показал, что они имеют общие закономерности функционирования. Каждый из рассмотренных алгоритмов работы средств аутентификации содержит этапы:

- обработки входных воздействий и преобразования их в необходимый вид;
- идентификации и аутентификации;
- принятия решения о разрешении доступа к защищаемой системе или его запрете;
- контроля исполнения управляющего воздействия.

Далее произведен обзор существующих методов оценки эффективности средств опознания субъектов. Описаны методы оценки эффективности средств опознания, основывающиеся на вероятностных и временных показателях, к которым относятся вероятность подбора аутентификатора и время безопасного использования аутентификатора. Данные показатели легко применимы для средств опознания первых двух классов, однако, значения характеристик, получаемых в процессе работы средства опознания по биометрическим признакам, всегда имеют разброс в небольшой области с некоторым

вероятностным распределением. Поэтому для принятия решения необходимо определять «окно применяемости» для каждого параметра. При экспериментальной оптимизации качества средства опознания размер окна может меняться, но он всегда остается больше некоторого минимума, так как для опознания по биометрическим признакам практически не существует абсолютно надежного набора параметров. Аналитические выражения для оценки эффективности биометрических средств опознания в известной литературе не приводятся, что обуславливает необходимость использования экспериментальных методов оценки.

Здесь же произведена постановка задач исследований, определяющая необходимость разработки обобщенной функциональной структуры средства аутентификации; выбора показателей эффективности средств аутентификации, учитывающих как их функциональные особенности, так и условия эксплуатации; определения методов формальной оценки показателей эффективности для биометрических средств аутентификации; синтеза математической модели средств аутентификации; разработки метода оценки средств аутентификации всех классов опознания в реальных условиях функционирования и определения требований по их проектированию.

Во второй главе, на основании обзора алгоритмов работы средств аутентификации всех классов опознания, произведено построение алгоритма работы типового средства аутентификации [1-А], блок-схема которого представлена на рисунке 1.

Функциональная структура средства аутентификации (рисунок 1) включает четыре основные функции, которые осуществляют свою работу в строго заданной последовательности. В зависимости от класса опознания, на основании которого построено средство аутентификации, содержание функций обнаружения, опознания, управления и контроля изменяется, но они обязательно присутствуют в том или ином виде в функциональной структуре любого из них.

Представленный на рисунке 1 алгоритм работы типовой структуры средства аутентификации позволяет описать работу средств аутентификации всех классов опознания.

Далее был сформулирован и доказан ряд утверждений, определяющих условия реализации средств аутентификации [2-А]:

– средства аутентификации относятся к классу средств защиты каналов доступа;

– необходимым и достаточным условием реализации средства аутентификации является наличие в его функциональной структуре совокупности функций обнаружения, опознания, управления и контроля;

– алгоритм работы средства аутентификации заключается в строгой последовательности выполнения функций обнаружения, опознания, управления и контроля;

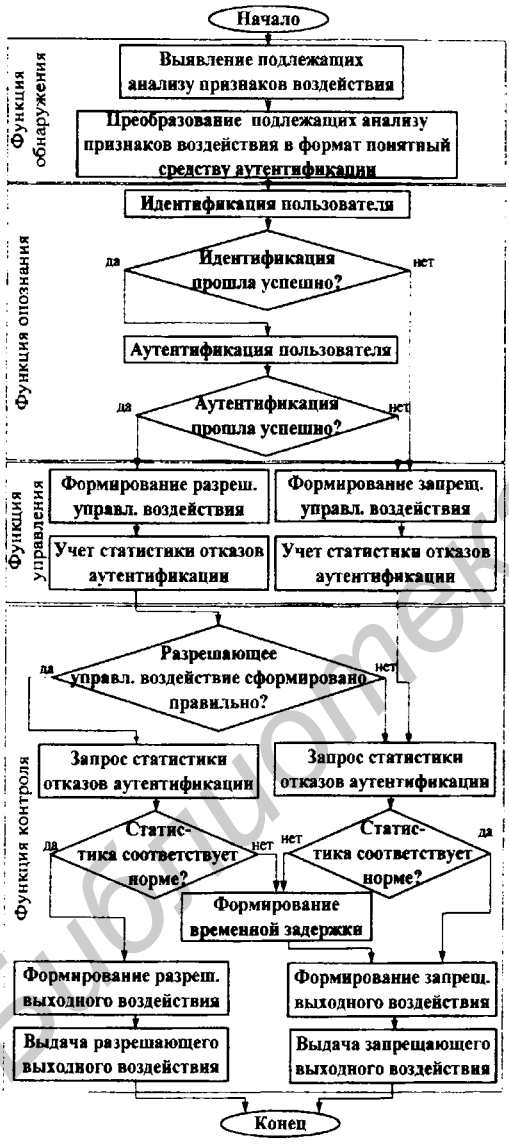


Рисунок 1 – Блок-схема алгоритма работы типового средства аутентификации

– средство аутентификации должно обеспечивать формирование выходного воздействия только при выполнении полного цикла работы.

Основной задачей средства аутентификации является надежное опознание личности конкретного человека. В соответствии с этим показатель эффективности средства аутентификации определен, как мера приближения вероятности правильного опознания субъекта данным средством в реальных условиях функционирования $P_{ПО}$ к требуемой $P_{ТР}$:

$$E = e^{-2\pi\cdot\Delta^2}, \qquad (1)$$

где E – эффективность средства аутентификации;

Δ – нормированная мера приближения $P_{ПО}$ к $P_{ТР}$.

Нормированная мера приближения $P_{ПО}$ к $P_{ТР}$ определяется выражением:

$$\Delta = 2\cdot 10^{\delta+1}\cdot(P_{ТР} - P_{ПО}), \qquad (2)$$

где δ – минимальное количество нулевых разрядов после запятой в мерах приближения $P_{ПО}$ к $P_{ТР}$.

Вероятность правильного опознания субъекта средством аутентификации в реальных условиях функционирования можно определить как:

$$P_{ПО} = (1 - P_{ПА}) \cdot (1 - P_{ОТ}) \cdot (1 - P_{ДН}), \quad (3)$$

где $P_{ПА}$ – вероятность подбора аутентификатора;

$P_{ОТ}$ – вероятность пропуска «чужого» в результате отказов (сбоев) оборудования;

$P_{ДН}$ – вероятность пропуска «чужого» в результате действий нарушителя.

Вероятность $P_{ПА}$ зависит от объёма алфавита, длины аутентификатора и является функцией числа попыток подбора:

$$P_{ПА} = 1 - \prod_{b=1}^{k} (1 - P_{ПАb}), \quad (4)$$

где k – число попыток подбора;

$P_{ПАb}$ – вероятность подбора аутентификатора с b-й попытки.

Вероятность $P_{ОТ}$ определяется надёжностью элементов средства аутентификации и является функцией интенсивности их отказов:

$$P_{ОТ}(\lambda) = 1 - e^{-\sum_{j=1}^{n} \lambda_{sj} t}, \quad (5)$$

где λ_{sj} – интенсивность отказов элементов, выполняющих s-ую функцию;

n – количество элементов, реализующих s-ую функцию.

Вероятность пропуска «чужого» в результате действия нарушителя вычисляется, как произведение вероятности того, что действие нарушителя было реализовано, и того, что оно привело к пропуску «чужого»:

$$P_{ДН} = P_{РДН} \cdot P_{ПДН}, \quad (6)$$

где $P_{РДН}$ – вероятность того, что действие нарушителя было реализовано;

$P_{ПДН}$ – вероятность того, что реализованное действие нарушителя привело к пропуску «чужого».

В качестве требуемой вероятности правильного опознания выбрана вероятность, дополняющая до единицы вероятность пропуска средством аутентификации «чужого» субъекта в результате подбора им аутентификатора с первой попытки:

$$P_{ТР} = 1 - P_{ПА1}, \quad (7)$$

Вероятность $P_{ПА1}$, а следовательно и вероятность $P_{ТР}$, определяется только конструктивными особенностями средства аутентификации, не зависит от внешних и внутренних негативных факторов и поэтому может служить верхней границей вероятности $P_{ПО}$.

Таким образом, эффективность средства аутентификации зависит как от характеристик самого средства аутентификации, так и от условий его функционирования.

Далее были определены подходы для формальной оценки требуемой вероятности правильного опознания для устройств аутентификации по отпечатку пальца и образцу голоса. Для этого были получены аналитические выражения для вычисления вероятности подбора аутентификатора с первой

попытки для данных биометрических средств аутентификации.

Для средства аутентификации по отпечатку пальца вероятность подбора аутентификатора с первой попытки определяется следующим аналитическим выражением [5-А]:

$$P_{ПА1} = \sum_{u=\text{int}(\sqrt{g \cdot p \cdot q})+1}^{\min(p,q)} (0{,}1373)^u , \qquad (8)$$

где p – количество минуций выделенных на изображении отпечатка пальца, предоставленного субъектом;

q – количество минуций выделенных на эталонном изображении отпечатка пальца;

g – порог меры близости изображений отпечатков пальцев;

u – количество совпавших пар минуций, которое изменяется от минимального целого значения, удовлетворяющего выражению

$$g = \frac{u^2}{p \cdot q},$$

до минимального значения из p или q.

При p = 10, q = 10 и g = 0,75 вероятность пропуска средством аутентификации «чужого» субъекта в результате подбора им аутентификатора с первой попытки составила $0{,}1972 \cdot 10^{-7}$.

Для средства аутентификации по образцу голоса вероятность подбора аутентификатора с первой попытки зависит от значений матриц мер близости и заданного порога меры близости [6-А]:

$$P_{ПА1} = \varphi(D_1, D_2, D_3, d), \qquad (9)$$

где D_1, D_2, D_3 – три матрицы мер близости (одинаковой размерности);

d – заданное значение порога меры близости.

Для нормирования порога и матриц мер близости была выбрана следующая функция нормирования:

$$f(x) = \frac{2}{\pi}\left|\text{arctg}(x)\right|. \qquad (10)$$

Вероятностью подбора аутентификатора с первой попытки для данного средства аутентификации является вероятность того, что в двух из трех дискретных нормированных матрицах мер близости найдется M значений, равных нормированному порогу меры близости Δ таких, что каждому столбцу и каждой строке данной матрицы будет принадлежать только одно из выбранных значений.

Формула вероятности подбора аутентификатора с первой попытки с учетом равенства размеров матриц мер близости имеет вид:

$$P_{ПА1} = 3 \cdot P_{\Delta}^2 \cdot (1 - P_{\Delta}) + P_{\Delta}^3, \qquad (11)$$

где P_Δ – вероятность того, что найдется хотя бы одно значение дискретной нормированной матрицы мер близости размерностью $i \times i$ равное Δ.

$$P_\Delta = \sum_{h=1}^{i^2} \frac{(i^2)!}{h!\cdot(i^2-h)!} \cdot \Delta^h \cdot (1-\Delta)^{(i^2-h)}, \qquad (12)$$

где i – переменная, значение которой равно количеству строк или столбцов квадратной матрицы меры близости; $i = M, M\text{-}1, \ldots, 1$;

M – количество интервалов времени в оцифрованных сигналах;

Δ – нормированное значение порога меры близости;

h – переменная, значение которой равно количеству ячеек в матрице размером $i \times i$; $h = 1,2,\ldots,i^2$.

При $M = 32$, $L = 14$ и $d = 0{,}05$ вероятность пропуска средством аутентификации «чужого» субъекта в результате подбора им аутентификатора с первой попытки составила $0{,}239 \cdot 10^{-7}$.

Полученные подходы можно использовать для вывода аналогичных выражений по расчету требуемой вероятности правильного опознания для других видов биометрических средств аутентификации.

В третьей главе производится синтез математической модели средств аутентификации и его реализация [3-А, 8-А].

Работа средства аутентификации представляется в виде вероятностного автомата, содержащего конечный набор состояний, в одном из которых он находится в каждый момент времени. Функционирование вероятностного автомата в каждом такте зависит только от предшествующего состояния и описывается вероятностным законом.

Графически процесс работы автомата, т.е. переходы из состояния в состояние, представляются в виде ориентированного графа. Вершины орграфа определяются состояниями, в которых может находиться автомат. Наличие ребра орграфа определяется наличием перехода между состояниями, которым соответствуют вершины, соединенные данной дугой. Причем, направление дуги определяет направление перехода из состояния в состояние автомата.

Обработка таким автоматом входного воздействия представляет собой последовательный обход ребер от начальной до конечной вершины, причем каждое ребро задействуется только один раз.

Таким образом, автоматное преобразование представляет собой цепь, которая в силу случайности входной последовательности может быть описана Марковской цепью.

Синтез модели средства аутентификации состоит из двух этапов:

– построение модели средства аутентификации функционирующего в идеальных условиях на основании описания алгоритма работы данного средства аутентификации;

– построение модели средства аутентификации функционирующего в условиях действия угроз путем введения в модель дополнительных состояний и враждебных переходов.

Построение модели средства аутентификации на первом этапе производится путем определения и композиции отдельных графов, соответствующих четырем функциям средства аутентификации [3-А].

Моделью средства аутентификации функционирующего в условиях действия угроз называется модель, которая описывает средство аутентификации в условиях воздействия внутренних и внешних факторов, приводящих к нарушению выполнения его функций. Данные факторы отображаются на графе модели новыми состояниями и враждебными переходами, которые соответствуют конкретным угрозам.

В качестве угроз рассматривались события, приводящие к переходу средства аутентификации из запрещающего состояния в разрешающее при запрещенном входном воздействии и из разрешающего состояния в запрещающее при разрешенном входном воздействии.

В качестве источников угроз рассматривались:

– отказы (сбои) в работе оборудования средства аутентификации;
– ошибки проектирования средства аутентификации;
– ошибки эксплуатации средства аутентификации.

Модель средства аутентификации функционирующего в условиях действия угроз так же строится путем композиции моделей его функций с учетом рассмотренных враждебных переходов.

На рисунке 2 представлен граф модели средства парольной аутентификации в ОС MS Windows XP функционирующего в условиях действия угроз [3-А].

Полученные математические модели исследуемых в работе средств аутентификации, учитывают особенности их функционирования и влияние угроз, приводящих к пропуску «чужого» субъекта или блокировке «своего».

Для реализации модели средств аутентификации были выбраны среда программирования Borland Delphi 7.0 и электронные таблицы MS Excel 2007.

С помощью программы модели средств аутентификации, реализованной в среде программирования Borland Delphi 7.0, были определены вероятности пропуска «чужого» при различных исходных данных [4-А].

Исходными данными для программы являются: 1) тип средства аутентификации; входное воздействие; 2) угрозы, действующие на выбранное средство аутентификации; 3) интенсивности отказов оборудования; 4) допустимое число попыток неверного входа в систему.

В результате обработки исходных данных строятся граф средства аутентификации и матрица переходов. Далее производится определение всех

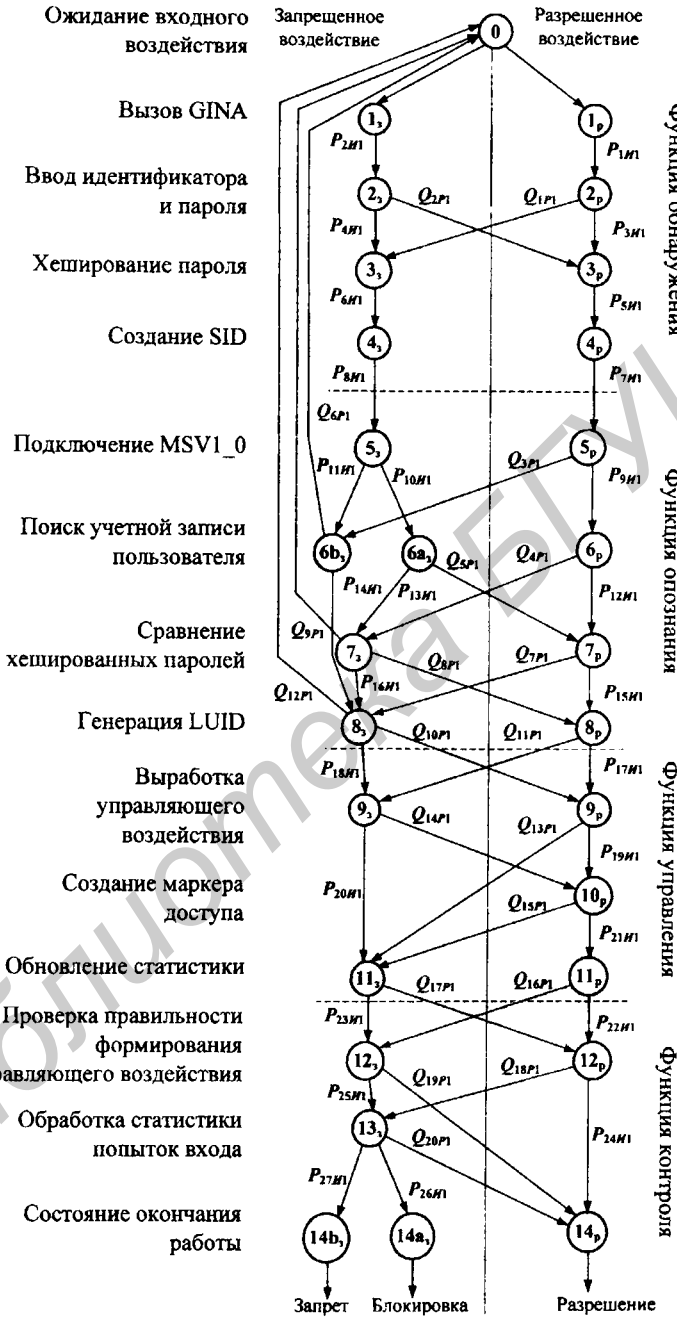


Рисунок 2 – Граф модели средства парольной аутентификации в ОС MS Windows XP функционирующего в условиях действия угроз

возможных вариантов путей прохода полученного графа от заданного входного воздействия к разрешающему или запрещающему выходным воздействиям, к начальному состоянию или к состоянию блокировки средства аутентификации.

Все полученные проходы разбиваются на соответствующие группы [4-А]. Затем, используя вероятности переходов из матрицы переходов, по формуле условной вероятности рассчитывается вероятность каждого из найденных проходов.

Результатом работы программы являются следующие вероятности:

– Вероятность пропуска «чужого» субъекта при запрещенном входном воздействии, которая определяется как сумма вероятностей всех проходов графа, при которых запрещенное входное воздействие приводит к разрешающему выходному.

– Вероятность блокировки «своего» субъекта при разрешенном входном воздействии, которая определяется как сумма вероятностей всех проходов графа, при которых разрешенное входное воздействие приводит к запрещающему выходному.

Далее, с использованием полученных значений вероятностей пропуска «чужого» субъекта или блокировки «своего» и исходных данных для определения вероятности подбора аутентификатора, производится расчет вероятностей правильного опознания для заданных значений интенсивности отказов по формуле (3).

Реализованная модель средств аутентификации позволяет исследовать поведение средств аутентификации в условиях воздействия на них случайных и преднамеренных угроз.

В четвертой главе представлены результаты исследования реализованной модели средств аутентификации, установлены основные принципы проектирования средств аутентификации, на основании которых разработаны и представлены требования к эффективным средствам аутентификации, а также метод по оценке их эффективности.

Исследования средств аутентификации проводились в следующем порядке:

Этап 1. По исходным данным определялась вероятность пропуска «чужого» в результате подбора им аутентификатора с первой попытки ($P_{\text{ПА1}}$). Величина, дополняющая $P_{\text{ПА1}}$ до единицы принималась в качестве верхней границы вероятности правильного опознания субъекта.

Этап 2. Для заданного числа разрешенных попыток входа в систему вычислялась вероятность подбора субъектом аутентификатора ($P_{\text{ПА}}$).

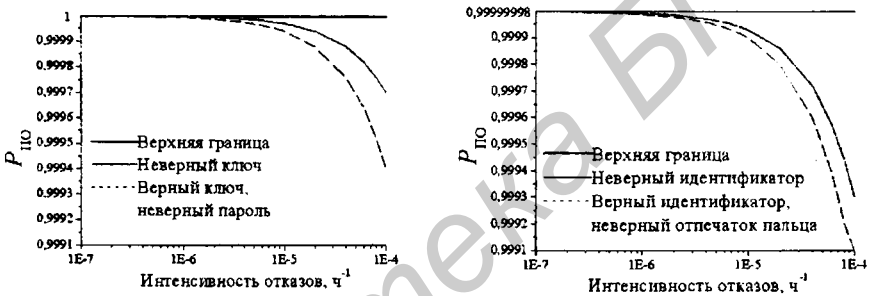
Этап 3. Для каждого из возможных запрещенных входных воздействий, задавалась интенсивность отказов оборудования при выполнении функций средства аутентификации и определялись вероятности пропуска «чужого».

Этап 4. Дополнительно к условиям второго этапа учитывались одиночные действия нарушителя. В результате определялись вероятности того, что реализованное действие нарушителя привело к пропуску «чужого» ($P_{\text{пдн}}$). Затем по формуле (6) определялась вероятность пропуска «чужого» в результате действия нарушителя ($P_{\text{дн}}$).

Этап 5. По результатам первых четырех этапов, с использованием формулы (3) вычислялась вероятность правильного опознания субъекта и, с использованием формулы (2), – эффективность средства аутентификации.

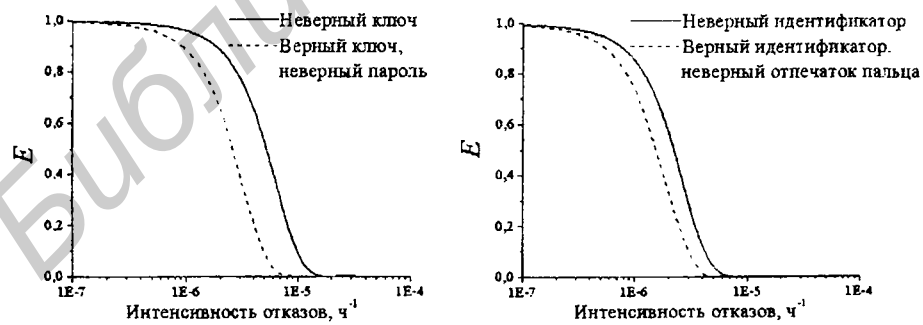
На рисунках 4 и 5 представлены результаты исследования средств аутентификации с использованием синтезированной модели.

Анализ результатов моделирования показывает, что конструкционные особенности и среда функционирования существенно снижают вероятность правильного опознания, а, следовательно, и эффективность средств аутентификации для всех классов опознания.



а б

Рисунок 4 – Зависимость вероятности правильного опознания от интенсивности отказов для средства аутентификации с использованием электронных ключей (а) и средства аутентификации по отпечатку пальца (б)



а б

Рисунок 5 – Зависимость эффективности от интенсивности отказов для средства аутентификации с использованием электронных ключей (а) и средства аутентификации по отпечатку пальца (б)

Разработка средств аутентификации должна основываться на принципах максимизации правдоподобия, ограничения попыток НСД и задания цикличности работы для обеспечения повышения вероятности правильного опознания субъектов.

На основании проведенных исследований и принципов проектирования средств аутентификации были сформулированы основополагающие требования к средствам аутентификации, которые должны соблюдаться при их проектировании, основными из которых являются:

1. В функциональной структуре средства аутентификации должны присутствовать функции обнаружения, опознания, управления и контроля.

2. Средство аутентификации в процессе функционирования должно обеспечивать выполнение функций обнаружения, опознания, управления и контроля в строгой последовательности.

3. Средство аутентификации должно полностью выполнять цикл указанных функций, не зависимо от результата работы каждой из них.

4. При отработке запрещенного входного воздействия или при превышении допустимого количества попыток неправильного входа в цикл работы средства аутентификации должна вносится существенная временная задержка.

5. При отсутствии входного воздействия на выходе средства аутентификации должно быть запрещающее выходное воздействие.

Метод оценки эффективности средства аутентификации включает в себя следующие этапы:

– формализация исследуемого средства аутентификации;

– анализ цикличности функциональной структуры средства аутентификации;

– оценка вероятностей событий, приводящих к нарушению работы;

– исследование параметров средства аутентификации на модели и оценка результатов исследования.

Данный метод оценки средств аутентификации позволяет с помощью синтезированной модели оценить эффективность средства аутентификации в реальных условиях эксплуатации.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

В диссертационной работе на основании проведенных теоретических и экспериментальных исследований автором получены следующие результаты.

1. Установлено, что функциональная структура средства аутентификации включает четыре основные функции: обнаружения, опознания, управления и контроля; а алгоритм его работы заключается в строгой последовательности

выполнения данных функций по установленному циклу. Представленный обобщенный алгоритм работы средства аутентификации позволяет описать работу средств аутентификации всех трех классов опознания, выделить в них этапы, выполняющие основные функции, и произвести построение их функциональной структуры [1-А, 7-А].

2. Показано, что эффективность средства аутентификации зависит как от его конструктивных параметров, так и от условий функционирования. В качестве показателя для оценки эффективности средств аутентификации всех трех классов опознания выбрана вероятность правильного опознания, значение которой зависит от вероятности подбора аутентификатора нарушителем, от вероятности выдачи разрешающего выходного воздействия в результате отказа (сбоя) оборудования и от вероятности выдачи разрешающего выходного сообщения в результате реализации действий нарушителя [4-А].

3. Определены подходы и представлены аналитические выражения для вычисления вероятности пропуска «чужого» средствами аутентификации по отпечатку пальца ($P_{\text{оп}} = 0{,}1972 \cdot 10^{-7}$) [5-А] и образцу голоса ($P_{\text{ог}} = 0{,}239 \cdot 10^{-7}$) [6-А]. Полученные подходы можно использовать для вывода аналогичных выражений по расчету вероятности пропуска «чужого» для других видов биометрических средств аутентификации.

4. Предложена математическая модель средств аутентификации, основанная на описании разрешенных и запрещенных состояний данного средства и вероятностных переходов между ними с использованием цепей Маркова. Процесс работы модели графически представлен в виде ориентированного графа, вершины которого определяются состояниями, в которых может находиться средство аутентификации, а наличие ребер орграфа определяется наличием переходов между состояниями [3-А, 8-А]. Исследовано поведение модели в условиях появления неисправностей оборудования с интенсивностью от 10^{-7} до 10^{-4} $ч^{-1}$ и воздействия нарушителя, вероятности реализации которых равны от 10^{-6} до 10^{-5}. Получены зависимости эффективности средств аутентификации трех классов опознания от интенсивности отказов оборудования и допустимого числа попыток неверного входа в систему [4-А]. Установлено, что при увеличении интенсивности отказов оборудования на порядок эффективность уменьшается на 15-20%, а при увеличении интенсивности отказов оборудования на два порядка – эффективность близка к нулю. На основе полученных результатов установлено, что конструкционные особенности и среда функционирования существенно снижают вероятность правильного опознания субъекта средством аутентификации по отношению к теоретической и, следовательно, их эффективность.

5. Показано, что разработка средств аутентификации для обеспечения повышения вероятности правильного опознания субъектов должна основываться на принципах максимизации правдоподобия, который для средств аутентификации первых двух классов опознания заключается в абсолютном совпадении всех сравниваемых признаков входного воздействия, а для средств аутентификации третьего класса – в минимизации значения меры близости сравниваемых признаков; ограничения попыток НСД, который заключается в ограничении числа попыток неправильного входа в систему; задания цикличности работы, который заключается в функционировании средства аутентификации по заранее установленному жесткому циклу с внесением временной задержки после каждой попытки неправильного входа в систему [2-А].

6. Разработан метод оценки средств аутентификации, включающий этапы формализации исследуемого средства и анализа его функциональной структуры [1-А], оценки вероятностей событий нарушения работы средства аутентификации и расчета вероятности правильного опознания [4-А], позволяющий с помощью синтезированной модели оценить эффективность средства аутентификации, используемого в сетях телекоммуникаций, в реальных условиях эксплуатации [3-А].

Основные положения диссертационной работы обсуждались на трех научно-технических конференциях и отражены в восьми печатных работах, из которых шесть статей.

Рекомендации по практическому использованию результатов

1. Метод оценки эффективности средств аутентификации использовался при выполнении проекта №25 «Создать единую информационную систему контроля за выполнением поручений Президента Республики Беларусь» в рамках Государственной программы информатизации Республики Беларусь на 2003 – 2005 годы и на перспективу до 2010 года «Электронная Беларусь», утвержденной Постановлением СМ РБ от 27.12.2002 г. №1819.

2. Разработанная модель средств аутентификации дает возможность производить оценку средств аутентификации в реальных условиях эксплуатации, что позволяет использовать ее для сертификационных исследований конкретных продуктов в области защиты информации [7-А].

3. Использование разработанной модели в совокупности с методами формального определения требуемой величины вероятности правильного опознания может значительно улучшить качество оценки средств аутентификации, используемых в сетях телекоммуникаций, и в результате сформировать требования по повышению эффективности средств аутентификации в процессе их проектирования [8-А].

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи

1-А. Буй, П. М. Типовые элементы структуры средства аутентификации / П. М. Буй, М. Н. Бобов // Доклады БГУИР. – 2006. – №6. – С. 40–47.

2-А. Буй, П. М. Защита информации в корпоративных сетях Белорусской железной дороги / П. М. Буй, М. Н. Бобов // Вестник БелГУТа: Наука и транспорт. – 2007. – №1-2 (14-15). – С. 140–143.

3-А. Бобов, М. Н. Синтез модели средства аутентификации / М. Н. Бобов, П. М. Буй // Доклады БГУИР. – 2007. – №5. – С. 23–31.

4-А. Буй, П. М. Исследование модели средств аутентификации / П. М. Буй // Доклады БГУИР. – 2007. – №5. – С. 32–38.

5-А. Бобов, М. Н. Оценка уровня защищенности средства аутентификации по отпечатку пальца // М. Н. Бобов, П. М. Буй // Управление защитой информации. – 2008. – № 1. – С. 58–64.

6-А. Бобов, М. Н. Оценка уровня защищенности голосового средства аутентификации / М. Н. Бобов, П. М. Буй // Информатика. – 2008. – № 1(17). – С. 31–37.

Материалы конференций

7-А. Буй, П. М. Модель средства защиты от НСД к информации в корпоративных сетях коммуикаций / П. М. Буй // Технические средства защиты информации: материалы докладов IV Белорусско-российской науч.-техн. конф., Минск – Нарочь, 29 мая – 2 июня 2006г. / Белорус. гос. ун-т информатики и радиоэлектроники; редкол.: М.П. Батура [и др.]. – Минск: БГУИР, 2006. – С. 50–51.

8-А. Буй, П. М. Идеальная модель средства аутентификации / П. М. Буй // Технические средства защиты информации: материалы докладов V Белорусско-российской науч.-техн. конф., Минск – Нарочь, 28 мая – 1 июня 2007г. / Белорус. гос. ун-т информатики и радиоэлектроники; редкол.: М.П. Батура [и др.]. – Минск: БГУИР, 2007. – С. 48–49.

Буй

РЭЗЮМЭ

Буй Павел Міхайлавіч

МЕТАД І СРОДКІ АДЗНАКІ ЭФЕКТЫЎНАСЦІ ЎСТРОЙСТВАЎ АЎТЭНТЫФІКАЦЫІ Ў СЕТКАХ ТЭЛЕКАМУНІКАЦЫЙ

Ключавыя словы: сродак аўтэнтыфікацыі, клас апазнання, біяметрыя, імавернасць вернага апазнання, матэматычная мадэль, ланцуг Маркава, арыентаваны граф, метад адзнакі эфектыўнасці.

Мэтай працы з'яўляецца комплекснае даследванне і распрацоўка метадаў адзнакі сродкаў аўтэнтыфікацыі, накіраваныя на павышэнне эфектыўнасці іх працы ў сетках тэлекамунікацый. **Аб'ектам** даследвання з'яўляюцца сродкі аўтэнтыфікацыі, якія выкарыстоўваюцца ў сетках тэлекамунікацый. **Прадметам** даследвання з'яўляецца эфектыўнасць сродкаў аўтэнтыфікацыі.

Асноўнымі **метадамі даследвання** з'яўляюцца метады тэорыі мностваў, тэорыі імавернасці, Маркаўскіх працэсаў, тэорыі графаў, а таксама тэхнічныя метады, якія ўключаюць камп'ютэрнае мадэліраванне.

Вынікамі працы з'яўляюцца: 1) Функцыянальная структура і абагульнены алгарытм працы сродкаў аўтэнтыфікацыі трох класаў апазнання. 2) Аналітычныя выражэнні для вылічэння імавернасці пропуску «чужога» сродкамі аўтэнтыфікацыі па адбітку пальца і ўзору голаса, якія дазваляюць выключыць значныя часовыя затраты на правядзенне іх эксперыментальных адзнак. 3) Матэматычная мадэль сродкаў аўтэнтыфікацыі, якая дазваляе вызначыць залежнасць эфектыўнасці даследуемых сродкаў аўтэнтыфікацыі ад інтэнсіўнасці сапсавання абсталяванняў, згодна якой, пры павеліченні інтэнсіўнасці сапсавання на парадак, эфектыўнасць сродкаў аўтэнтыфікацыі памяншаецца на 15-20%. 4) Метад адзнакі эфектыўнасці сродкаў аўтэнтыфікацыі, які дазваляе ўстанавіць ступень выканання патрэбных паказацелей з улікам пэўнай рэалізацыі сродкаў аўтэнтыфікацыі і рэальных умоў іх эксплуатацыі.

Распрацаваную мадэль сродкаў аўтэнтыфікацыі можна **рэкамендаваць да выкарыстоўвання** для сертыфікацыйных даследванняў пэўных прадуктаў у сферы аховы інфармацыі, а таксама, у сукупнасці з метадамі фармальнай адзнакі патрэбных паказацелей эфектыўнасці, яна можа значна палепшыць якасць адзнакі сродкаў аўтэнтыфікацыі, якія выкарыстоўваюцца ў сетках тэлекамунікацый.

Вынікі працы знайшлі скарыстанне пры ўтварэнні адзінай інфармацыйнай сістэмы кантролю за выкананнем даручэнняў Прэзідэнта Рэспублікі Беларусь (праект №25 Дзяржаўнай праграмы інфарматызацыі Рэспублікі Беларусь на 2003 – 2005 гг і на перспектыву да 2010 года «Электронная Беларусь»).

РЕЗЮМЕ

Буй Павел Михайлович

МЕТОД И СРЕДСТВА ОЦЕНКИ ЭФФЕКТИВНОСТИ УСТРОЙСТВ АУТЕНТИФИКАЦИИ В СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ

Ключевые слова: средство аутентификации, класс опознания, биометрия, вероятность правильного опознания, математическая модель, цепь Маркова, ориентированный граф, метод оценки эффективности.

Целью работы является комплексное исследование и разработка метода оценки средств аутентификации, направленные на повышение эффективности их работы в сетях телекоммуникаций. **Объектом** исследования являются средства аутентификации, используемые в сетях телекоммуникаций. **Предметом** исследования является эффективность средств аутентификации.

Основными **методами исследования** являются методы теории множеств, теории вероятности, Марковских процессов, теории графов, а также технические методы, включающие компьютерное моделирование.

Результатами работы являются: 1) Функциональная структура и обобщенный алгоритм работы средств аутентификации трех классов опознания. 2) Аналитические выражения для вычисления вероятности пропуска «чужого» средствами аутентификации по отпечатку пальца и образцу голоса, позволяющие исключить значительные временные затраты на проведение их экспериментальных оценок. 3) Математическая модель средств аутентификации, позволяющая определить зависимость эффективности исследуемых средств аутентификации от интенсивности отказов оборудования, согласно которой, при увеличении интенсивности отказов на порядок, эффективность средств аутентификации уменьшается на 15-20%. 4) Метод оценки эффективности средств аутентификации, позволяющий установить степень выполнения требуемых показателей с учетом конкретной реализации средств аутентификации и реальных условий их эксплуатации.

Разработанную модель средств аутентификации можно **рекомендовать к использованию** для сертификационных исследований конкретных продуктов в сфере защиты информации, а также, в совокупности с методами формальной оценки требуемых показателей эффективности, она может значительно улучшить качество оценки средств аутентификации, используемых в сетях телекоммуникаций.

Результаты работы нашли **применение** при создании единой информационной системы контроля за выполнением поручений Президента Республики Беларусь (проект №25 Государственной программы информатизации Республики Беларусь на 2003 – 2005 годы и на перспективу до 2010 года «Электронная Беларусь»).

SUMMARY

Bui Pavel Mihailovich

A METHOD AND TOOLS OF THE EFFECTIVENESS ESTIMATION OF THE AUTHENTIFICATION DEVICES IN TELECOMMUNICATIONS NETWORKS

Key words: the authentification tool, the class of an identification, the biometry, the probability of a correct identification, the mathematical model, the Markov circuit, the focused of columns, the efficiency estimation method.

The complex research and working out of an estimation of the authentification tools method, directed at increasing of effectiveness of their work in telecommunications networks, are **the purpose of the work**. The authentification tools, which are used in telecommunications networks, are **a research object**. The effectiveness of authentification tools **is a research subject**.

The theory of sets, the theory of probability, the Markov processes, the columns theory methods, and technical methods including also computer modeling, are the basic **research methods.**

The results of the work are: 1) The functional structure and generalized algorithm of authentification tools work of three identification classes. 2) The analytical expressions for the calculation of the passing "enemy" probability by authentification tools by a fingerprint and a voice model. These expressions allow to exclude large temporary expenses for carrying out experimental estimations of authentification tools. 3) The mathematical authentification tool model. This model allows to receive dependence of the authentification tools effectiveness from equipment fault intensity. The authentification tools effectiveness decreases on 15-20% at increasing fault intensity ten times. 4) The authentification tools effectiveness estimation method. This method allows to state fulfillment degree of the required effectiveness parameters. The method takes into account the concrete realizations of authentification tools and the real conditions of their function.

The developed authentification tools model can be **recommended to use** for certified researches of the some products in the field of information protection. This model can considerably improve quality of the authentification tools estimation, used in the telecommunications networks, with methods of the formal estimation of required effectiveness parameters.

The results of the work have **found an use** at creating the uniform information monitoring system for carrying out the President of Republic of Belarus orders (project №25 The Republic of Belarus state program of information on 2003 – 2005 and in future till 2010 "Electronic Belarus").

Научное издание

БУЙ Павел Михайлович

МЕТОД И СРЕДСТВА ОЦЕНКИ ЭФФЕКТИВНОСТИ УСТРОЙСТВ АУТЕНТИФИКАЦИИ В СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать 19.05.2008. Формат 60x84 1/16. Бумага офсетная.
Гарнитура «Таймс». Печать ризографическая. Усл. печ. л. 1,4.
Уч.-изд. л. 1,2. Тираж 60 экз. Заказ 297.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0056964 от 01.04.2004. ЛП №02330/0131666 от 30.04.2004.
220013, Минск, П. Бровки, 6