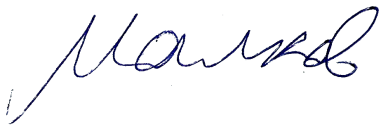
На правах рукописи



МАЛКОВ Анатолий Александрович

ТЕХНОЛОГИЯ АУТЕНТИФИКАЦИИ С ПОМОЩЬЮ ДОВЕРЕННЫХ ЛИЦ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Уфа – 2013

Работа выполнена на кафедре прикладной физики ФГОБУ ВПО «Пермский национальный исследовательский политехнический университет»

Научный руководитель: д-р физ.-мат. наук, доцент **Кротов Лев Николаевич**

Официальные оппоненты: доктор технических наук, профессор **Васильев Владимир Иванович,** ФГОБУ ВПО «Уфимский государственный авиационный технический университет», зав. кафедры вычислительной техники и защиты информации

кандидат технических наук, доцент, **Марчук Александр Васильевич,** советник дирекции по научно-техническому комплексу госкорпорация «Росатом», г. Москва

Ведущее предприятие: **ЗАО «Прогноз»**, г. Пермь

Защита диссертации состоится «01» ноября 2013 г. в 10:00 часов на заседании диссертационного совета Д-212.288.07 при Уфимском государственном авиационном техническом университете в актовом зале 1-го корпуса по адресу: 450000, г. Уфа, ул. К. Маркса, 12

С диссертацией можно ознакомиться в библиотеке Уфимского государственного авиационного технического университета.

Автореферат разослан «__» сентября 2013 года

Ученый секретарь
диссертационного совета
д-р техн. наук, доцент И. Л. Виноградова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. С начала пятой информационной революции прошло всего несколько десятков лет, но за это время информатизация общества достигла невиданного доселе размаха. Информационные технологии проникли практически во все сферы человеческой деятельности. Практически у каждого человека, живущего в этом информационном обществе, есть по несколько учётных записей в различных информационных системах. Его учётная запись есть в базе данных его личного или рабочего компьютера, на почтовом или файлообменном сервере, на интернет-сайте или в социальной сети. И ценность данных, относимых к этим записям, со временем только увеличивается. Соответственно, с каждым годом растёт и спрос на различные средства защиты информации. Вслед за ним растут усилия злоумышленников, желающих эти средства защиты преодолеть. Это соревнование “меча и щита”, “снаряда и брони” будет продолжаться ещё долго, а потому разработка новых средств и систем информационной безопасности не потеряет своей актуальности, по крайней мере, до следующей информационной революции.

Степень разработанности темы. В последнее время проникновение интернет-технологий в нашу жизнь достигло таких масштабов, что стало возможным построение новых систем аутентификации, ранее технически неосуществимых. Представленная работа посвящена такой системе, относящейся к самому нераспространённому и малоизученному из методов аутентификации пользователей – социальной аутентификации, интерес к которой в последние годы заметно вырос. Это внимание вызвано взрывным ростом количества пользователей социальных сетей и сети Интернет. Опубликованные исследования по указанной теме можно пересчитать по пальцам одной руки. Наибольший вклад в её развитие на данный момент внесли 3 коллектива исследователей из RSA Laboratories (John Brainard, Ari Juels, Michael Szydlo, Moti Yung и др.), Microsoft (Stuart Schechter, Serge Egelman, Serge Egelman) и Facebook. Учитывая всё выше сказанное, актуальность диссертационной работы не вызывает сомнений.

Исследование было выполнено при поддержке гранта РФФИ-Урал 11-01-96015-р_урал_а.

Объект исследования

– методы и алгоритмы аутентификации пользователей;

– методы оценки качества;

– модель процесса аутентификации.

Предмет исследования – технологии социальной аутентификации, основанные на использовании доверенных лиц.

Целью работы является повышение эффективности системы социальной

аутентификации путём автоматизации сбора и анализа оценок доверенных лиц.

Задачи исследования:

1. На основании анализа существующих методов аутентификации предложить классификацию технологий аутентификации пользователей.
2. Разработать математическую модель процесса социальной аутентификации.
3. Разработать метод оценки качества систем социальной аутентификации.
4. Разработать прототип автоматизированной системы восстановления доступа к учётной записи, основанный на технологии социальной аутентификации с помощью доверенных лиц.
5. Оценить качество разработанного прототипа системы восстановления доступа к учётной записи.

Научная новизна работы заключается в следующем**:**

1. Предложена фасетная классификация технологий аутентификации пользователей в информационной системе, основанная на таких существенных признаках, как степень автоматизации системы аутентификации, приоритет использования механизма аутентификации и используемый фактор аутентификации, позволяющая оценить адекватность используемых технологий аутентификации и соответствие их требованиям защищённости.
2. Разработана математическая модель процесса социальной аутентификации, позволяющая по заданному числу допустимых неудовлетворительных оценок вычислить вероятность успешной аутентификации с использованием метода вычисления времени премодерации, позволяющего восстанавливать пароль как при его утере, так и его смене злоумышленником, и метода анализа оценок поручителей на основе теории нечетких множеств, позволяющего проводить аутентификацию пользователей с помощью малого числа доверенных лиц с различной степенью компетентности.
3. Предложен метод оценки качества систем социальной аутентификации на основе ГОСТ 28195-89, отличающийся использованием новой номенклатуры показателей качества, таких как удобство пользователя, затратность и защищённость (первый уровень), затраты пользователя на аутентификацию, качество аутентификации, качество доверенного канала связи, качество интерфейса, легкость освоения и др. (второй уровень), финансовые затраты, лёгкость освоения, уровень автоматизации и др. (третий уровень), время аутентификации, простота предварительной настройки, наличие веб-интерфейса центра авторизации и др. (четвёртый уровень), что позволяет получить интегральную оценку качества системы социальной аутентификации.
4. Разработан алгоритм работы автоматизированной системы восстановления доступа к учётной записи, основанный на технологии социальной аутентификации с помощью доверенных лиц, при которой решение о

восстановлении доступа принимается на основании оценок поручителей, отличающийся от существующих аналогов наличием проверки доверенных каналов связи на этапе формирования списка поручителей, анализом активности пользователя за период времени, предшествующий обращению к системе, путём вычисления времени премодерации, возможностью для поручителей выставлять отрицательные оценки уверенности в личности пользователя, идентификацией инициатора запуска системы с помощью номера сеанса восстановления доступа, и составом данных, передаваемых пользователю в списке поручителей.

Теоретическая и практическая ценность полученных результатов состоит в том, что разработанный прототип автоматизированной системы восстановления доступа к учётной записи:

1. Отличается повышенными показателями вероятности успешной аутентификации для легального пользователя в случае утери пароля до 0,97, а в случае смены пароля злоумышленником до 0,9.
2. Практически неуязвим к автоматизированным атакам, снижает вероятность успеха неперсонализированной атаки до 0,00009, а персонализированной до 0,004, атаки со стороны близкого знакомого до 0,032, со стороны поручителя до 0,198 и со стороны группы поручителей до 0,35.
3. Снижает на 30% трудозатраты сотрудников отделов информационной безопасности и подразделений технической поддержки на поддержку пользователей.
4. Обладает возможностью интеграции в подсистему управления доступом информационной системы, имеющей доступ к доверенным каналам связи с поручителями и использующей парольную аутентификацию.

Разработанное программное обеспечение “Центр Авторизации” внедрено в компании системного интегратора ЗАО “БИОНТ”, г. Пермь.

Методология и методы исследования. В работе использована методология структурного анализа и проектирования информационных систем, методы кластерного анализа, математический аппарат теории вероятностей и математической статистики, теории нечётких множеств, методы экспертного оценивания, теории массового обслуживания и математического моделирования.

Положения, выносимые на защиту:

1. Классификация технологий аутентификации пользователей, основанная на учёте степени автоматизации, приоритета использования и факторов аутентификации.
2. Математическая модель процесса социальной аутентификации на основе оценок доверенных лиц.
3. Метод оценки качества систем социальной аутентификации на основе предложенной 4-х уровневой номенклатуры показателей качества.
4. Прототип автоматизированной системы восстановления доступа к

учётной записи на основании оценок доверенных лиц.

Достоверность полученных результатов основана на использовании известных теоретических подходов, математических методов и моделей. Достоверность и обоснованность выводов и результатов, полученных в работе, подтверждена результатами моделирования разработанной системы восстановления доступа к учётной записи с использованием реальных данных, а также соответствием результатов теоретических и экспериментальных исследований.

Апробация результатов. Основные положения диссертации докладывались и обсуждались на международных и всероссийских научно-технических конференциях:

- II Международной научной конференции «Тенденции и перспективы развития современного научного знания», Москва, 2012 г.;
- III Международной научно-практической конференции «Интеграция науки и практики как механизм эффективного развития современного общества», Москва, 2012 г.;
- Международной научно-практической конференции «Теория и практика актуальных исследований», Краснодар, 2012 г.

Получен патент на полезную модель “Автоматизированная система социальной аутентификации последней инстанции”, № RU 121946 U1 от 10.11.2012.

Публикации. Основные положения и результаты опубликованы в 8 печатных работах, в том числе 3 работы опубликованы в изданиях, вошедших в перечень ВАК, получен патент на полезную модель.

Структура и объем диссертации. диссертация состоит из введения, четырёх глав, заключения и списка литературы. Диссертация содержит 148 страниц машинописного текста. Список литературы включает 64 наименования, 32 таблицу и 25 рисунков. Библиографический список содержит 64 наименования.

Благодарности. Автор выражает глубочайшую благодарность к.ф.-м.н. Кротовой Е.Л. за неоценимую помощь и поддержку на всех этапах работы над диссертацией.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность разработки автоматизированных систем восстановления паролей, с помощью доверенных лиц. Сформулированы цель работы, задачи, определены научная новизна и практическая значимость результатов.

В первой главе рассматриваются существующие методы аутентификации их сильные и слабые стороны. В параграфе 1.1 механизмы анализируются в зависимости от факторов, используемых в процессе аутентификации. Так,

“фактор знания” используется в системах, основанных на вводе пароля или ответа на секретный вопрос. На “вещественном факторе” базируются все системы защиты, в которых применяются такие электронные идентификаторы, как USB-ключи, смарт-карты, радиочастотные идентификаторы, идентификаторы iButton и другие е-токены. “Биофактор” применяется в биометрических системах распознавания отпечатков пальцев, геометрии руки, радужной оболочки глаза, голоса, лица, почерка и т.п. К системам, использующим “социальный фактор”, относятся, например, службы поддержки пользователей, которые позволяют получить доступ к учётной записи пользователя после его разговора с оператором. В параграфе 1.2 методы анализируются с точки зрения приоритета их использования. Так, основные методы аутентификации используются для штатного входа в систему. В случае потери пароля или взлома учётной записи имеется возможность вернуть доступ, используя резервные механизмы, такие как доверенный почтовый ящик. Самые надёжные из резервных механизмов, а так же те, что требуют вмешательства со стороны администраторов информационной системы, получили название last-resort, что можно перевести как последнее средство или механизмы последней инстанции. В параграфе 1.3 формулируются требования, к разрабатываемой математической модели автоматизированной системы социальной аутентификации последней инстанции. Описываются критерии её оценки.

Вторая глава начинается с рассмотрения простейшего алгоритма работы такой системы, из которого становится понятно, что его реализуемость зависит от того, будут ли разработаны методы вычисления времени премодерации и оценки границы доверия.

В параграфе 2.1 дано описание математической модели социальной аутентификации. Пусть у нас есть три основных класса объектов:

- S – некая информационная система, имеющая в своём составе подсистему разграничения доступа, реализующую технологию аутентификации с помощью доверенных лиц, которую мы будем называть Центром Авторизации CA;
- User — пользователь, человек имеющий учётную запись в ИС S;
- Voucher — поручитель, человек способный подтвердить личность пользователя.

В процессе аутентификации поручители должны подтвердить в ЦА личность пользователя. С помощью описания модели, нужно определить основные параметры системы, такие как вероятности успешной аутентификации.

Обозначим известные величины:

- $a_i = \{e_0^i, e_1^i, .., e_n^i\}$ — аутентификатор, некая совокупность информации и её носителя, описываемая (n+1) мерным вектором, где e_0^i – автор/владелец, а $\{e_1^i, .., e_n^i\}$ - множество лиц, которым известен этот аутентификатор;
- $A = \{a_i\}, i \in N$ - множество всех аутентификаторов;

- $priv(x) = \{a_i \in A \mid e_0^i = x\}$ - функция, определяющая аутентификаторы, принадлежащие объекту x;
- $know(x) = \{a_i \in A \mid \exists j = \overline{1,n} : e_j^i = x\}$ - функция, определяющая аутентификаторы, известные объекту x, но не принадлежащие ему;
- Voucher_k — k-й поручитель, человек способный подтвердить личность пользователя, т.е. тот кто обладает и/или знает о аутентификаторах, принадлежащих или известных пользователю;
- $Z_k = (priv(User) \cup know(User)) \cap (priv(Voucher_k) \cup know(Voucher_k))$, (1)
множество аутентификаторов, которые можно использовать при проверке личности пользователя k-ым поручителем;
- $f_{auth}(User, Voucher_k, a_i) = \begin{cases} 1, User'(a_i) \propto Voucher_k'(a_i) \in [k_{\min}; k_{\max}]; \\ 0, User'(a_i) \propto Voucher_k'(a_i) \notin [k_{\min}; k_{\max}]. \end{cases}$, (2)
функция аутентификация, проверяющая степень подобия образов аутентификатора, имеющихся у пользователя и k-го поручителя, где $a_i \in Z_k$ и $k_{\min}, k_{\max} \in [0;1]$ - границы строгости аутентификации;

В таблице 1 описана вербально-числовая шкала Харрингтона, содержащая описание градаций шкалы и числовые значения, соответствующие каждой из градаций шкалы, имеет широкое применение, универсальный характер и позволяет измерить степень интенсивности критериального свойства, имеющего субъективный характер. Отмечу, что численные значения градаций шкалы Харрингтона получены на основе анализа и обработки большого массива статистических данных.

Таблица 1. Шкала Харрингтона.

Числовое значение	Оценка, данная поручителем (est^c)
0,05	c = 1 – “полностью уверен, что не он”
0,175	c = 2 – “уверен, что не он”
0,325	c = 3 – “кажется, что не он”
0,5	c = 4 – “не знаю”
0,675	c = 5 – “кажется, что он”
0,825	c = 6 – “уверен, что он”
0,95	c = 7 – “полностью уверен, что он”

$$f_{\text{Harrington}}(x) = \begin{cases} \text{est}^1, \text{x} \in (0;0.1]; \\ \text{est}^2, \text{x} \in (0.1;0.25]; \\ \text{est}^3, \text{x} \in (0.25;0.4]; \\ \text{est}^4, \text{x} \in (0.4;0.6]; \\ \text{est}^5, \text{x} \in (0.6;0.75]; \\ \text{est}^6, \text{x} \in (0.75;0.9]; \\ \text{est}^7, \text{x} \in (0.9;1]; \end{cases}, \quad (3)$$

- функция преобразующая числовое значение в одну из градаций порядковой шкалы Харрингтона.

$$F_{\text{Harrington}}(est^c) = \begin{cases} 0.05, c = 1; \\ 0.175, c = 2; \\ 0.325, c = 3; \\ 0.5, c = 4; \\ 0.675, c = 5; \\ 0.825, c = 6; \\ 0.95, c = 7; \end{cases}, \quad (4)$$

- функция преобразующая градацию порядковой шкалы Харрингтона в числовое значение.

Обозначим неизвестные величины:

P_w — вероятность успешной аутентификации на основании w оценок;

Модель состоит из ИС, пользователя, поручителей, а также множества аутентификаторов. В качестве входного параметра выступает идентификатор пользователя, в качестве выходного параметра, либо новый пароль от учётной записи, либо отказ в восстановлении доступа.

Пользователь проходит CAPTCHA с вероятностью p_1 после чего отправляет в Центр авторизации (ЦА), идентификатор своей учётной записи, доступ к которой нужно восстановить:

$User \to \{Login\} \to CA$

Центр авторизации (ЦА) генерирует временную учётную запись (ВрУЗ), и передаёт пользователю логин Ns и пароль $Pass_{time}$, где в качестве логина выступает номер сеанса восстановления пароля (СВП), получающийся путём добавления случайного числа в диапазоне от 2 до 5 к номеру предыдущего СВП $Ns = Ns_0 + random[2;5]$:

$CA \to \{Ns, Pass_{time}\} \to User$

Центр авторизации (ЦА), вычисляет время премодерации t_{pr} .

Далее, ЦА выясняет разницу времени между последней сменой пароля пользователя T_{reset} и моментом создания ВрУЗ, и если она больше времени премодерации $T_{reset} + t_{pr} < T_0$, то высылает легальному пользователю информационное сообщение о запуске системы и ждёт ответа с запросом на прекращение процедуры восстановления пароля, получив который система прекращают свою работу с данным сеансом.

Если же ответа от легального пользователя так и не последовало или $T_{reset} + t_{pr} \geq T_0$, то ЦА передаёт пользователю перечень ников, содержащийся в списке поручителей $List_{\text{vouchers}} = \{(x, y, b^1, b^2)\}$ действительном на момент $T_0 - t_{pr}$, содержащий ники $x \in \{Name\}$, доверенные каналы связи $y \in \{0;1;2\}$ (0 – электронный почтовый адрес, 1 – номер телефона, 2 – учётная запись в социальной сети), отношение пользователя $b^1 \in \{B_1^1, B_2^1, B_3^1\}$ и объем общения с поручителем $b^2 \in \{B_1^2, B_2^2, B_3^2\}$:

$CA \to \{x_{\text{vouchers}}\} \to User$

Причём p_2 - вероятность получения списка поручителей, а p_3 - вероятность определения поручителя на основании полученных данных.

Затем ЦА рассылает всем поручителям из списка информационное сообщение, в котором содержится просьба связаться с легальным пользователем лично, по телефону, либо по другому доверенному каналу связи и узнать номер его СВП. В сообщении также описана методика проверка личности пользователя.

Получив список поручителей, пользователь пытается связаться с каждым из них. В случае успеха, он просит их помочь ему восстановить доступ к своей учётной записи, сообщает номер своего СВП и необходимую для подтверждения своей личности информацию $User'(Z'_k)$, где $Z'_k = \{j = \overline{1,J} : a_j\} \subseteq Z_k$, а $p_3(t)$– вероятность связаться с поручителем за время t:

$$User \rightarrow \{Ns, User'(Z'_k)\} \rightarrow Voucher_k, k = \overline{1,K}$$

Получив пользовательские образы аутентификаторов, поручитель сравнивает их, с имеющимися у себя, и пытается, с помощью вербально-числовой шкалы Харрингтона, оценить количество информации содержащейся в аутентификаторах, прошедших проверку, по сравнению с общим количеством, а затем передаёт в ЦА оценку est_k, номер СВП и способ проверки $b^3 \in \{B_1^3, B_2^3, B_3^3\}$:

$$est_k = f_{\text{Harrington}}\left(\frac{\sum\limits_{a_j \in Z'_k} H(a_j) * f_{auth(User, Voucher_k, a_j)}}{\sum\limits_{a_j \in Z'_k} H(a_j)}\right); \qquad (5)$$

$$Voucher_k \rightarrow \{Ns, est_k, b^3\} \rightarrow CA$$

Причём, p_4 – вероятность получения оценки, а $p_5(b_3, est_{border})$ – вероятность получения положительной оценки, зависящая от способа проверки личности пользователя b_3 и границы доверия est_{border}, - величины отделяющей удовлетворительные оценки от неудовлетворительных.

Получив очередную оценку, Центр авторизации (ЦА), вычисляет компетентность k-го поручителя η_k, который в данной ситуации выступает в качестве эксперта. Компетентность поручителя зависит от их основных характеристик, таких как: отношение и объём общения с пользователем, а также способ проверки его личности, которые определяются на основании ответов $B_m^n = \{B_m^n, m = \overline{1, M^n}\}$ на множество вопросов $D = \{D^n, m = \overline{1,N}\}$. Так как ответы даны в порядковой шкале, то каждому из них, согласно таблице 2, соответствует положительный нормированный коэффициент $\rho_m^n \in [0;1]$, причём $\sum\limits_{m=1}^{M^n} \rho_m^n = 1$:

$$\eta_k = \frac{\sum\limits_{n=1}^{3} \eta_k^n}{\sum\limits_{n=1}^{3} \max_m \rho_m^n}, \qquad (6)$$

где $\eta_k^n \in [0;1]$ - нормированный коэффициент ответа k-го поручителя на n-й вопрос.

Таблица 2. Сравнительная таблица вопросов-ответов с нормированными коэффициентами.

	B_1	B_2	B_3
D^1 : "Кем поручитель приходится пользователю?"	"Коллега" $\rho_1^1 = 1/6$	"Друг" $\rho_2^1 = 2/6$	"Родственник" $\rho_3^1 = 3/6$
D^2 : "Объем общения с пользователем?"	"Слабо" $\rho_1^2 = 1/6$	"Достаточно" $\rho_2^2 = 2/6$	"Тесно" $\rho_3^2 = 3/6$
D^3 : "Способ проверки личности пользователя поручителем?"	"Опрос по переписке" $\rho_1^3 = 1/6$	"Телефонный разговор" $\rho_2^3 = 2/6$	"Личная встреча" $\rho_3^3 = 3/6$

С помощью операции "размывания", уровень компетентности будет влиять на нечёткую количественную меру, в качестве которой будет выступать оценка поручителя est_k:

$$\tilde{\mu}_k = F_{\text{Harrington}}(est_k)^{\eta_k}, \quad (7)$$

В результате, в ЦА имеется множество нечётких количественных мер ψ, учитывающих компетентность поручителей, в которое не входит минимальная из имеющихся оценок $\psi = \{\min\{\tilde{\mu}_k\} \notin \{\tilde{\mu}_k\}\}$. Эта мера используется для борьбы с атаками злоумышленников, путём повышения робастности модели. Следовательно, нечёткое множество, характеризующееся обобщённым мнением группы поручителей, можно определить как пересечение нечётких мнений поручителей. Общая оценка в таком случае будет равна:

$est = \min \psi$

Если общая компетентность поручителей превышает минимально необходимый вес поручителей η_{border} ($\sum_{k=1}^{K} \eta_k > \eta_{border}$), а общая оценка превышает границу доверия $\text{est}_{\text{border}}$ ($est \geq est_{border}$), то аутентификация считается успешно пройденной и Центр авторизации (ЦА) высылает пользователю на его ВрУЗ новый пароль от его учётной записи:

$CA \rightarrow \{Pass_{new}\} \rightarrow User$

Чему будут равны неизвестные величины? Так как вероятности p_1, p_2, p_3, p_4 и p_5 независимы друг от друга по своей природе, то согласно биномиальному закону:

$$P_{legal}(t, est_{border}, v, w) = p_1 p_2 C_w^v (p_3 p_4 p_5)^{w-v} ((1-p_3) + p_3(1-p_4) + p_3 p_4 (1-p_5))^v, \quad (8)$$

- вероятность для пользователя получить v – отрицательных оценок из w – общего количества полученных оценок поручителей, где

$$C_w^v = \frac{w!}{v!(w-v)!}, \quad (9)$$

- количество комбинаций. Так как для увеличения робастности было решено считать аутентификацию успешной даже в случае получения одной неудовлетворительной оценки, то вероятность успешной аутентификации равна:

$$P_w(t, est_{border}, w) = P_{legal}(t, est_{border}, 1, w) + P_{legal}(t, est_{border}, 0, w) =$$

$$= p_1 p_2 \cdot (C_w^1 (p_3 p_4 p_5)^{w-1} ((1-p_3) + p_3(1-p_4) + p_3 p_4 (1-p_5)) + C_w^0 (p_3 p_4 p_5)^w) =, \quad (10)$$

$$= p_1 p_2 \cdot (w(p_3 p_4 p_5)^{w-1} ((1-p_3) + p_3(1-p_4) + p_3 p_4 (1-p_5)) + (p_3 p_4 p_5)^w)$$

Параграф 2.2 посвящён разработке метода вычисления времени премодерации. На первом этапе оно описывается как период времени, в течение которого легальный пользователь, почти наверняка, воспользуется своей учётной записью, т.е. период времени, за который пользователь успеет заметить, что он забыл свой пароль или его учётную запись взломали, соответственно, действия совершенные в этот временной интервал от его лица, вероятно, принадлежат злоумышленнику.

Параграф 2.3 посвящен границе доверия, т.е. некоему условию, согласно которому будет определяться личность пользователя. Согласно разработанному алгоритму работы системы аутентификации, проверке на соответствие этому условию будут подвергаться оценки поручителей, отражающие их мнение о личности испытуемого. Задача заключалась в поиске граничных значений двух параметров: границе доверия $est_{border,}$ оценки превышающие которую будут считаться удовлетворительными, и минимальной общей компетентности η_{border} .

В одной из опубликованных работ приводятся интересные данные о том, что из более чем четырёхсот респондентов каждый сумел точно ответить как минимум на 70% вопросов, что соответствует оценке “5” из таблицы 1. Таким образом, доверительный интервал при опросе по переписке будет в диапазоне от 5 до 7 баллов или от 60% до 100% верных ответов. Соответственно, границу доверия можно считать равной $est_{border} = 0{,}6$.

Согласно исследованию С. Шехтера, С. Игельмана и П. Б. Ридера от 2009 года, достаточно надёжным является поручительство как минимум 3-х человек (члена семьи, друга по учёбе, друга по работе). А т.к. компетентность одного поручителя не может превысить единицу, по определению, то их общая компетентность должна превышать 2 ($\sum_{k=1}^{K} \eta_k > 2$), т.е. минимально необходимое количество поручителей будет находиться в диапазоне от трёх до семи, в зависимости от их компетентности.

В третьей главе подробно описана работа комплекса программ, реализующих базовый алгоритм АС САПИ, которую можно условно разделить на 4 этапа.

1. *Подготовительный этап*. На этом этапе в Центре Авторизации (ЦА) составляется список экспертов-поручителей, которые могут подтвердить личность легального пользователя, в который включаются: доверенные каналы связи с поручителями, например, электронные адреса, номера телефонов, учётные записи в интернет-пейджерах или социальных сетях и т.п.; компетенция поручителей, в виде весовых коэффициентов, вычисляющаяся на основе ответов на несколько вопросов, или на основе имеющейся о пользователе информации; по желанию, может быть добавлен комментарий пользователя, который будет отправлен поручителю при запросе подтверждения.

На доверенный канал высылается запрос, после подтверждения, которого он добавляется в список поручителей.

1. *Запуск системы*. Как только пользователь понимает, что лишился доступа к своей учётной записи, он должен сообщить об этом в ЦА.

2.1. После прохождения пользователем системы защиты от ботов ЦА создаёт сеанс восстановления пароля (СВП). А также создаётся временная учётная запись, именем для которой служит номер СВП. Пароль от этой временной учётной записи (ВрУЗ) сообщается пользователю.

2.2. Вычисление времени премодерации для данного пользователя, т.е. периода времени, в течение которого легальный пользователь с очень высокой вероятностью должен воспользоваться своей учётной записью:

- анализ активности пользователя за достаточно длительный период (от нескольких месяцев до года), при необходимости возможно применение плотностных алгоритмов кластеризации, типа, DBSCAN;
- вычисление времени премодерации $\tau = \frac{\ln N}{\lambda}$, где λ - плотность потока обращений, а N – количество сеансов активности учётной записи за исследуемый период.

2.3. Проверка активности пользователя за период времени $(T_o - \tau; T_o)$, где T_o - время обращения в ЦА.

- Если в течение этого периода времени пароль на учётную запись был изменён, то это служит косвенным доказательством взлома учётной записи и достаточным основанием для передачи пользователю списка экспертов, причём изменения, произведённые с учётной записью в период времени $(T_o - \tau; T_o)$, считаются не вступившими в силу.

- Если же пароль не менялся, то ЦА, исходя из предположения о том, что пользователь просто забыл или потерял пароль, посылает легальному пользователю сообщение, в котором говорится о том, что в ЦА поступило обращение с просьбой восстановить права на эту учётную запись и ЦА просит разрешить или запретить проведение процедуры восстановления. В случае если за время премодерации прошедшее с момента отправки сообщения, ЦА так и не получил ответа, то это служит косвенным подтверждением слов пользователя и на этом основании ему передаётся список экспертов.

После этого ЦА сам посылает сообщения всем экспертам-поручителям из списка, с описанием сложившейся ситуации и просьбой связаться с легальным пользователем, используя доверенный канал связи, например, лично или по телефону. Так же в сообщении могут иметься более подробные инструкции и рекомендации по проверке личности пользователя.

3. *Получение экспертных оценок*. Получив список экспертов, пользователь связывается с каждым из них и описывает свою проблему. Также пользователь сообщает каждому из поручителей номер своего СВП. После этого эксперт может обратиться в ЦА, где должен будет указать: способ аутентификации пользователя согласно таблице 2; степень уверенности в личности пользователя по шкале оценок поручителей согласно таблице 1; номер СВП пользователя.

4. *Анализ экспертных оценок*. После регистрации достаточного количества оценок, ЦА анализирует их достоверность и достаточность.

Сперва вычисляется компетентность каждого поручителя $\eta_k = \frac{\sum_{n=1}^{3} \eta_k^n}{\sum_{n=1}^{3} \max_m \rho_m^n}$ (11),

где $\eta_k^n \in [0;1]$ - нормированный коэффициент ответа k-го поручителя на n-й вопрос. Вербальные оценки поручителей est_k переводятся согласно шкале Харрингтона в числа, а затем размываются $\tilde{\mu}_k = F_{\text{Harrington}}(est_k)^{\eta_k}$. Для повышения робастности алгоритма исключается наименьшее значение $\psi = \{\min\{\tilde{\mu}_k\} \notin \{\tilde{\mu}_k\}\}$. Общая оценка будет равна наименьшему из оставшихся значений $est = \min \psi$. Если общая компетентность поручителей превышает 2 ($\sum_{k=1}^{K} \eta_k > 2$), а общая оценка превышает границу доверия $\text{est}_{\text{border}} = 0{,}6$ ($est \geq est_{border}$), то аутентификация считается успешно пройденной и Центр авторизации (ЦА) высылает пользователю на его ВрУЗ новый пароль от его учётной записи.

Кроме того, на языке UML подробно описан состав ПО, реализующий

алгоритм АС САПИ, механизмы взаимодействия компонентов между собой, с пользователями и информационными системами.

В параграфах 3.2 и 3.3 рассмотрены другие модификации этого алгоритма. А именно универсальная модификация САПИ-У, которую можно использовать практически в любой информационной системе, имеющей доступ к доверенным каналам связи с поручителями, но которая в свою очередь требует предварительной настройки со стороны легального пользователя. В системах же, имеющих доступ к некоторой персональной информации пользователя можно использовать САПИ-С – модификацию для социальных сетей.

Параграф 3.4 полностью посвящён оценке системы по всем основным критериям и сравнению её с действующими аналогами и прототипами.

В четвёртой главе подробно описана методика оценки систем социальной аутентификации (ССА). Параграф 4.1 посвящён самой методике вычисления показателей качестав ССА. В следующем параграфе схематично описана структура показателей качества, включая факторы качества удобство для пользователя, затратность и защищённость, делящиеся на критерии качества затраты пользователя на аутентификацию, качество аутентификации, универсальность доверенных каналов связи, качество интерфейса, легкость освоения, затраты администратора на установку, затраты на сопровождение, уровень автоматизации, временная эффективность, ресурсоёмкость, качество защиты и устойчивость к атакам. Далее подводятся итоги оценки разработанной системы по описанной методике показавшей его превосходство над аналогами по фактору удобство для пользователя на 13%, затратность на 28% и защищённость в 3,06 раза.

Параграф 4.5 посвящён оценке вероятностей успешной аутентификации. Для легального пользователя в зависимости от количества необходимых оценок, в случае потери пароля она будет находиться в диапазоне от 0,828 до 0,967, а в случае смены пароля злоумышленником от 0,717 до 0,902. Также были вычислены вероятности успешной аутентификации для семи различных математических моделей воздействия нарушителей. Все нарушители должны последовательно пройти основные этапы атаки, включающие: прохождение CAPTCHA, получение списка поручителей, определение каналов связи с поручителями и получение удовлетворительной оценки. Модели злоумышленников отличаются друг от друга вероятностями прохождения каждого из этапов, и зависят от типа используемой атаки. Вероятности успеха автоматизированных атак (АА), неперсонализированных полуавтоматизированных атак (НПА), неперсонализированных неавтоматизированных атак (ННА), персонализированных атак (ПА), атак со стороны близкого знакомого (АСБЗ), атак со стороны поручителя (АСП) и атак со стороны группы поручителей (АСГП), на

учётную запись активного пользователя, а также основные параметры моделей злоумышленников перечислены в таблице 3, а вероятности успеха атак на неактивную учётную запись в таблице 4.

Таблица 3. Вероятность успешной аутентификации для различных типов атак на активные учётные записи.

	АА	НПА	ННА	ПА	АСБЗ	АСП	АСГП
p_1 – вероятность успешно пройти CAPTCHA	0,1	1	1	1	1	1	1
p_2 – вероятность получить список поручителей	0,05	0,1	0,1	0,2	0,25	0,3	0,35
p_3 – вероятность определить поручителя и связаться с ним	0	0,1	0,1	0,3	0,5	0,7	0,9
p_4 – вероятность получить оценку от поручителя	0,5	0,6	0,6	0,7	0,8	0,85	0,95
p_5 – вероятность получить удовлетворительную оценку	0,045	0,045	0,29	0,4	0,56	0,7	0,8
P_3	0	2,2E-06	0,00009	0,004	0,032	0,198	0,35
P_7	0	2,7E-16	1,9E-11	4,6E-07	0,00018	0,015	0,173

Таблица 4. Вероятность успешной аутентификации для различных типов атак на неактивные учётные записи.

	АА	НПА	ННА	ПА	АСБЗ	АСП	АСГП
p_1 – вероятность успешно пройти CAPTCHA	0,1	1	1	1	1	1	1
p_2 – вероятность получить список поручителей	1	1	1	1	1	1	1
p_3 – вероятность определить поручителя и связаться с ним	0	0,1	0,1	0,3	0,5	0,7	0,9
p_4 – вероятность получить оценку от поручителя	0,5	0,6	0,6	0,7	0,8	0,85	0,95
p_5 – вероятность получить удовлетворительную оценку	0,045	0,045	0,29	0,4	0,56	0,7	0,8
P_3	0	2,2E-5	0,0009	0,02	0,128	0,66	1
P_7	0	2,7E-15	1,9E-09	2,3E-06	0,0007	0,049	0,5

В заключении сформулированы основные результаты работы.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Предложена фасетная классификация технологий аутентификации пользователей в информационной системе, основанная на таких существенных признаках, как степень автоматизации системы аутентификации, приоритет использования механизма аутентификации и используемый фактор аутентификации, позволяющая оценить адекватность используемых технологий аутентификации и соответствие их требованиям защищённости.

2. Разработана математическая модель процесса социальной аутентификации, позволяющая по заданному числу допустимых неудовлетворительных оценок вычислить вероятность успешной аутентификации с использованием метода вычисления времени премодерации, позволяющего восстанавливать пароль как при его утере, так и его смене злоумышленником, и метода анализа оценок поручителей на основе теории нечетких множеств, позволяющего проводить аутентификацию пользователей с помощью малого числа доверенных лиц с различной степенью компетентности.

3. Предложен метод оценки качества систем социальной аутентификации на основе ГОСТ 28195-89, отличающийся использованием новой номенклатуры показателей качества, таких как удобство пользователя, затратность и защищённость (первый уровень), затраты пользователя на аутентификацию, качество аутентификации, качество доверенного канала связи, качество интерфейса, легкость освоения и др. (второй уровень), финансовые затраты, лёгкость освоения, уровень автоматизации и др. (третий уровень), время аутентификации, простота предварительной настройки, наличие веб-интерфейса центра авторизации и др. (четвёртый уровень), что позволяет получить интегральную оценку качества системы социальной аутентификации.

4. Разработан прототип автоматизированной системы восстановления доступа к учётной записи, основанный на технологии социальной аутентификации с помощью доверенных лиц, при которой решение о восстановлении доступа принимается на основании оценок поручителей, отличающийся от существующих аналогов наличием проверки доверенных каналов связи на этапе формирования списка поручителей, анализом активности пользователя за период времени, предшествующий обращению к системе, путём вычисления времени премодерации, возможностью для поручителей выставлять отрицательные оценки уверенности в личности пользователя, идентификацией инициатора запуска системы с помощью номера сеанса восстановления доступа, и составом данных, передаваемых пользователю в списке поручителей.

5. Проведённая оценка качества разработанного прототипа автоматизированной системы восстановления доступа к учётной записи показала что его применение позволяет повысить по сравнению с аналогами удобство для пользователя на 13%, затратность на 28% и защищённость в 3.06 раза, обеспечивая практически полную неуязвимость к массированным не персонализированным атакам.

Перспективы дальнейшей разработки темы. Перспективными направлениями для дальнейших исследований являются уточнение параметров модели с помощью данных полученных во время испытаний рабочего прототипа.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах, вошедших в перечень ВАК

1. Малков А.А., Кротова Е.Л., Кротов Л.Н. Принцип работы экспертных систем для восстановления паролей от учетных записей в социальных сетях// Вестник ИжГТУ, изд-во ИжГТУ, №4, 2011. С. 145 – 147.

2. Малков А.А., Кротов Л.Н., Кротова Е.Л. Численные методы анализа экспертных оценок в системах социальной аутентификации// Системы управления и информационные технологии, Воронеж, Изд-во «Научная книга», №1(47), 2012. С. 62-65.

3. Малков А.А., Кротов Л.Н., Кротова Е.Л. Поиск оптимального времени премодерации в автоматизированных системах социальной аутентификации последней инстанции// Перспективы науки, №2(29), Тамбов, 2012. С.73-77.

4. Автоматизированная система социальной аутентификации последней инстанции / А.А. Малков // Патент на полезную модель № RU 121946 U1, опубл. 10.11.2012 г.

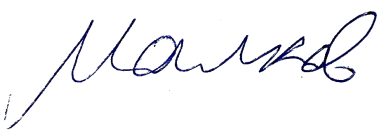
В других изданиях

5. Малков А.А., Кротов Л.Н., Кротова Е.Л. Оценка времени премодерации в автоматизированных системах социальной аутентификации// Информационные технологии моделирования и управления; Воронеж, Изд-во «Научная книга», №1(73) 2012, С.21-28. (РИНЦ)

6. Малков А.А. Принципы работы автоматизированных систем социальной аутентификации последней инстанции // Тенденции и перспективы развития современного научного знания: Материалы II международной научной конференции, Науч.-инф. издат. центр «Институт стратегических исследований». – Москва : Изд-во «Спецкнига», 2012. С. 70 – 72.

7. Малков А.А. Поиск оптимального метода вычисления времени премодерации в автоматизированных системах социальной аутентификации последней инстанции // Интеграция науки и практики как механизм эффективного развития современного общества: Материалы III международной научно-практической конференции, Науч.-инф. издат. центр «Институт стратегических исследований». – Москва : Изд-во «Спецкнига», 2012. С. 50 – 51.

8. Малков А.А. Описание математической модели социальной аутентификации // Теория и практика актуальных исследований: Материалы Международной научной конференции : Сборник научных трудов. – Краснодар, 2012. В 2-х томах. Т. 2. С. 278 – 279.

Диссертант  А.А. Малков