чаются или не различаются предъявляемые частоты, анализирует одновременно предъявляемые частоты мельканий, что не требует обращения к кратковременной логико-смысловой памяти. В результате точность определения полосы пропускания рецептивных полей нейронов зрительного анализатора увеличивается.

Заключение

Предложен способ определения полосы пропускания рецептивных полей нейронов зрительного анализатора, позволяющий повысить точность измерений. По результатам экспериментальных исследований точность измерений с использованием двух светодиодов по сравнению с использованием одного светодиода повышается по группе из 10 испытуемых от 19 до 34 %.

Библиографические ссылки

1. *Вартанян И. А.* Физиология сенсорных систем : руководство. – СПб. : Лань, 1999. – 224 с.

2. Зрение / А. И. Богословский [и др.] // Большая медицинская энциклопедия : в 30 т. – 3-е изд. – М. : Советская энциклопедия, 1978. – Т. 8. – С. 479–485.

3. *Шелепин Ю. Е.*, *Колесникова Л. Н.*, *Левкович Ю. И.* Визоконтрастометрия: Измерение пространственных передаточных функций зрительной системы. – Л. : Наука, 1985. – 103 с.

4. *Глезер В. Д.* Зрение и мышление. – Изд. 2-е, испр. и доп. – СПб. : Наука, 1993. – 284 с.

5. *Bishop P. O.*, *Coombs J. S.*, *Henry G. H.* Interaction effects of visual contours on the discharge frequency of simple neurons // J. Physiol. – 1971. – Vol. 219. – No. 3. – P. 659–687.

6. *Куперман А. М.* Анализ пространственных частотных характеристик сложных рецептивных полей // Биофизика. – 1977. – Т. 22. – Вып. 1. – С. 117–122.

7. Патент 2209028 РФ, МКИ А61В 3/00. Способ определения полосы пропускания рецептивных полей нейронов зрительной системы / В. В. Роженцов, Т. А. Лежнина. – Опубл. 27.07.2003, Бюл. № 21. – 4 с.

8. Патент 2347520 РФ, А61В 3/00, А61F 9/00, А61В 5/00, А61В 5/16. Способ определения полосы пропускания рецептивных полей нейронов зрительной системы / Роженцов В. В. – Опубл. 27.02.2009, Бюл. № 6.

9. Патент 2164778 РФ, А61В 5/16, 3/06. Способ оценки критической частоты слияния световых мельканий / В. В. Роженцов. – Опубл. 10.04.2001, Бюл. № 10.

10. СНиП 23–05–95. Естественное и искусственное освещение. Строительные нормы и правила Российской Федерации. – М. : Изд-во стандартов, 1995. – 30 с.

V. V. Rozhentsov, Doctor of Technical Sciences, Professor, Mari State Technical University

Study of Pass Band of Visual System Neuron Receptive Fields

The method of pass band (in Hz)determination of the visual analyzer neurons receptive fields by simultaneous presentation of incremental and decremental light flickers frequencies using two sources is proposed. According to experimental data, accuracy of pass band determination using two sources in comparison with conventional use of a single source is improved from 19 % to 34 % in a group of 10 testees.

Key words: neuron, receptive field, pass band.

УДК 004.9

Л. Н. Кротов, доктор физико-математических наук, профессор, Пермский государственный технический университет
Е. Л. Кротова, кандидат физико-математических наук, Пермский государственный технический университет
А. А. Малков, аспирант, Пермский государственный технический университет

ПРИНЦИП РАБОТЫ ЭКСПЕРТНЫХ СИСТЕМ ДЛЯ ВОССТАНОВЛЕНИЯ ПАРОЛЕЙ ОТ УЧЕТНЫХ ЗАПИСЕЙ В СОЦИАЛЬНЫХ СЕТЯХ

Описаны существующие системы восстановления прав в информационных системах и предложен простейший вариант экспертной системы, удовлетворяющий принципиально новым требованиям защиты.

Ключевые слова: математическое моделирование, информационная безопасность, аутентификация, автоматическое управление.

Любая информационная система (ИС) имеет в своем составе подсистему управления доступом, предназначенную для защиты от злоумышленников. Именно с этой целью на каждого пользователя заводится учетная запись, содержащая сведения о его привилегиях при пользовании системой, информацию, которую он сообщает о себе, включая набор данных для своей идентификации, как правило, пароль, пару «секретный вопрос – ответ», доверенные почтовые адреса или номера телефонов. Причем если пароль используется для входа в систему и авторизации пользователя, то секретный вопрос и доверенный адрес нужны в случае восстановления утерянного пароля. При взломе учетной записи ситуация усложняется тем, что злоумышленник может сменить все эти данные, после чего вернуть права легальному пользователю без вмешательства администраторов ресурса станет невозможно.

При ближайшем рассмотрении существующих систем восстановления прав на учетную запись ока-

Получено 27.06.11

зывается, что их немного. Перечислим основные методы. Первый и самый старый – это наличие секретного вопроса, ответ на который, как подразумевается, знает только пользователь (например, девичья фамилия матери или любимое блюдо). Лет двадцать назад это был очень эффективный метод. На сегодняшний момент специалисты требуют очень серьезно подходить к выбору секретного вопроса, и допустимые ранее варианты, как номер паспорта, строка из любимого литературного произведения и т. п., не рассматриваются как достаточно надежные, поскольку атака «brute force» позволит подобрать верный вариант из специального словаря за сравнительно небольшой промежуток времени. В наше время использование подобного метода не обеспечивает необходимой надежности системы.

Второй способ заключается в указании специального доверенного электронного почтового ящика, на который в случае необходимости будет выслан новый пароль. Недостатки этого метода очевидны. Во-первых, криптостойкость одной учетной записи напрямую зависит от криптостойкости доверенного электронного почтового ящика. Во-вторых, доверенным почтовым ящиком зачастую пользуются реже, чем самой учетной записью, поэтому вероятность забыть от него пароль тоже велика.

Третий способ лишен этих недостатков, так как в данном случае пароль высылается в виде SMS-сообщения на мобильный телефон. Данный метод широко распространен в системах «банк – клиент». Его недостатки тоже очевидны, как со стороны владельцев социальных сетей, которым необходимо иметь SMS-шлюз, так и со стороны пользователей, которым это грозит потерей анонимности, к тому же злоумышленник, временно завладев телефоном пользователя, может получить полный доступ к его учетной записи.

Хотя стремительный рост социальных сетей и их важности наблюдается уже давно, системы восстановления прав на учетные записи не претерпели никаких изменений. Поэтому мы решили разработать принципиально новую систему восстановления прав (СВП) на учетные записи специально для социальных сетей.

В отличие от систем, существующих в настоящее время, пользователь в случае утери пароля или взлома учетной записи должен иметь возможность восстановить права на свою учетную запись независимо от того, помнит ли он ответ на секретный вопрос и есть ли у него доверенный почтовый ящик или мобильный телефон. При этом система должна работать без вмешательства со стороны администраторов ИС.

Но как в таком случае ИС сможет идентифицировать личность пользователя, если он никак не может ее подтвердить? Тогда его личность должны подтвердить люди, хорошо знающие пользователя, кому он доверяет. Например, те, с кем он часто общался в данной социальной сети. Логично предположить, что те, с кем он много общался, и знают его лучше всех. В дальнейшем этих людей мы будем называть экспертами, а их мнения относительно личности пользователя – экспертными оценками.

Рассмотрим теперь, как будет выглядеть простейшая схема работы СВП, удовлетворяющая всем указанным требованиям.

1. *Подготовительный этап*

На этом этапе пользователь составляет список экспертов, которые могут подтвердить его личность. Этот список будет храниться в центре авторизации (ЦА), так мы будем называть ПО, отвечающее за реализацию СВП.

2. *Запуск СВП*

Как только пользователь понимает, что лишился доступа к своей учетной записи, он должен сообщить об этом в ЦА. После чего ЦА вычислит время премодерации для данного пользователя, т. е. период времени, в течение которого легальный пользователь с очень высокой вероятностью должен воспользоваться своей учетной записью. Если в течение этого периода времени, предшествующего данному обращению, пароль на учетную запись был изменен, то это служит косвенным доказательством взлома учетной записи и достаточным основанием для передачи пользователю списка экспертов. 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 учетную 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 передается список экспертов.

После этого ЦА сам посылает сообщения всем экспертам из списка с описанием сложившейся ситуации и просьбой связаться с легальным пользователем, желательно используя не данную социальную сеть, а другой доверенный канал связи.

3. *Получение экспертных оценок*

Получив список экспертов, пользователь связывается с каждым из них и описывает свою проблему. После этого эксперт может обратиться в ЦА, который попросит его оценить уверенность в личности пользователя по 7-балльной шкале [1]. 1 будет соответствовать «полностью уверен, что не он»; 4 – «не знаю»; 7 – «полностью уверен, что он». *Оценка будет зашифрована симметричным ключом, соответствующим паре «пользователь – эксперт», и к ней будет добавлена служебная информация, все это в дальнейшем мы будем называть частичным файл-ключом (ЧФК). Таким образом, никто кроме эксперта и ЦА не будет знать экспертную оценку.*

Получив ЧФК, эксперт может передать его пользователю. Пользователь, собрав необходимое число ЧФК, может передать их в ЦА.

4. *Анализ экспертных оценок*

После получения всех ЧФК ЦА анализирует оценки экспертов и проверяет, не превышают ли они границу доверия. Граница доверия – это некое усло-

вие, согласно которому будет определяться личность пользователя. В случае положительного результата ЦА генерирует новый пароль на учетную запись и передает его пользователю.

Эффективность данной системы определяется методами вычисления времени премодерации и границы доверия.

Граница доверия

При измерениях чего-либо *люди пользуются шестью* видами шкал:

1) шкала наименований (номинальная);
2) порядковая шкала (или ранговая);
3) интервальная шкала;
4) шкала отношений;
5) шкала разностей;
6) абсолютная шкала.

В случае когда человека просят оценить что-либо, он может сделать это, лишь используя порядковую шкалу, соответственно, и оценки экспертов будут относиться к этой шкале [2]. И здесь возникает главный вопрос: каких оценок экспертов будет достаточно, чтобы пользователь мог вернуть себе доступ к своей учетной записи? При этом необходимо учитывать, что далеко не каждый легальный пользователь сможет получить наивысшие оценки от всех экспертов. Более того, необходимо предусмотреть какой-то механизм, увеличивающий робастность системы, *защищающий ее от злоупотреблений со стороны злоумышленника, который может оказаться в числе экспертов.* Самым разумным будет проверить, удовлетворяют ли оценки экспертов какому-либо распределению, а так как оценки даются для порядковой шкалы, то для нее существует только одно так называемое универсальное гиперболическое ранговое распределение, или частотная структура типа Ципфа – Мандельброта [3].

Пусть количество экспертных оценок в 7 баллов равно C_1, в 6 баллов – C_2 и т. д. Согласно данному закону проверка будет считаться пройденной, если будет выполняться набор условий:

$$\begin{cases} C_1 \geq 2C_2, \\ C_1 \geq 3C_2, \\ C_1 \geq 4C_2, \\ C_1 \geq 5C_2, \\ C_1 \geq 6C_2, \\ C_1 \geq 7C_2. \end{cases}$$

Из условий видно, что робастность системы увеличивается с ростом числа экспертов.

Время премодерации

Время премодерации – это период времени, в течение которого легальный пользователь почти наверняка воспользуется своей учетной записью, т. е. период времени, за который пользователь успеет заметить, что он забыл свой пароль, его учетную запись взломали, либо ему пришло сообщение от ЦА.

Заметим, что оценка времени премодерации не может основываться на математическом аппарате цепей Маркова, так как условие марковости процесса не выполняется.

Наиболее ***простой*** способ вычисления времени премодерации с заданной вероятностью можно описать так.

1. Берется выборка наблюдений за некоторый период времени (например, несколько месяцев) использования учетной записи.

2. На основании наблюдений строится модифицированная выборка из интервалов времени между посещениями пользователя.

3. На основании вариационного ряда строится таблица $2 \times n$, в первом столбце указывается время, а во втором – соответствующий уровень ошибки первого рода α (в процентах, который вычисляется по формуле $100 - \frac{100n}{x}$). Таким образом, задав значение уровня значимости, например, 5 %, по таблице можно определить соответствующее время премодерации.

Библиографические ссылки

1. *Miller G.* The Magical Number Seven, Plus or Minus Two: Some Limits on or Capacity for Processing Information // Psychological Review. – 1956. – P. 81–97.

2. *Орлов А. И.* Устойчивость в социально-экономических моделях. – М. : Наука, 1979. – 296 с.

3. *Орлов Ю. К.* Обобщенный закон Ципфа – Мандельброта и частотные структуры информационных единиц различных уровней // Вычислительная лингвистика. – М. : Наука, 1976. – С. 179–202.

L. N. Krotov, Doctor of Physical and Mathematical Sciences, Professor, Perm State Technical University
E. L. Krotova, Candidate of Physical and Mathematical Sciences, Professor, Perm State Technical University
A. A. Malkov, Postgraduate Student, Perm State Technical University

Principle of Operation of Expert Systems for Restoration of Accounts Passwords in Social Networks

The existing systems of restoration of rights in information systems are described. An elementary variant of an expert system which meets principally new protection requirements is offered.

Key words: mathematical modeling, information security, authentification, automatic control.