втратах, тимчасових витратах, обсязі знищеної чи "зіпсованої" інформації і т. д.

Однак, практично це зробити дуже важко, особливо на ранніх етапах проектування СБІТ. Тому доцільно замість абсолютного збитку використовувати відносний збиток, що по суті являє собою ступінь небезпеки *i*-ї загрози для інформаційно-управляючої системи. Ступінь небезпеки може бути визначений експертним шляхом у припущенні, що всі загрози для ІТС складають повну групу повідомлень [3], тобто

$$0 \le \Delta qi \le 1; \sum_{i=1}^{n} \Delta qi = 1 .$$

Найбільш складним питанням є визначення імовірності усунення *i*-й загрози $\mathrm{P}i_{угр}^{устр}$ при проектуванні СБІТ. Зробимо природне допущення, що ця імовірність визначається тим, наскільки повно враховані якісні і кількісні вимоги до СБІТ при їх проектуванні, тобто

$$\mathrm{P}i_{угр}^{устр} = \gamma i(xi1,..,xi\gamma,..,xim), \qquad (7)$$

де $xi\gamma$ – ступінь виконання *i*-й вимоги до СБІТ для усунення її загрози, $i = 1,\overline{n}; \gamma = 1,\overline{m}$.

Таким чином, перевага НМ полягає в можливості описувати та обробляти множини зі змінним ступенем належності без урахування різноманітних комбінацій. З практичного погляду методи НМ допомагають експертам формалізувати свої знання зрозумілою для них мовою.

Отже, розроблення методів, технологій, моделей і систем безпеки інформації, які з використанням математичного апарату нечітких множин дозволяють ефективно впроваджувати захищені інформаційні технології, є актуальним науковим завданням. Дослідження цієї проблеми дозволить визначити методичні шляхи створення ефективних систем безпеки ІТ, які раціонально об'єднують різноманітні за властивостями засоби, заходи і методи захисту інформації.

Література: ***1.*** *Кофман А. Введение в теорию нечетких множеств М.: Радио и связь, 1982 - 432 с.* ***2.*** *Поспелова Д. А. Нечеткие множества в моделях управления и искусственного интелекта - М. :Наука, 1986 - 312 с.* ***3.*** *Борисов А. Н., Алексеев А. В., Меркурьев Г. В. и др. Обработка нечеткой информации в системах принятия решений-М: Радио и связь, 1989 - 304 с.* ***4.*** *Домарев В. В. Безопасность информационных технологий. Системный подход. – К.: ООО ТИД Диа Софт, 2004. – 992 с.*

УДК 681.3.06

БЕЗОПАСНОСТЬ ПАРОЛЬНОЙ ЗАЩИТЫ ПРИ РАЗЛИЧНЫХ МЕТОДАХ ВЗЛОМА

Сергей Емельянов

Международный гуманитарный университет, г. Одесса

Анотація: **Розглянуто основні фактори, що визначають безпеку парольного захисту. Наведено практичні рекомендації щодо посилення парольного захисту як від силового, так і від «інтелектуального» зламу.**

Summary: **Basic factors, which determine safety of password defense, are considered in this article. Practical recommendations are resulted in relation to strengthening of password defense both from power one and from a «intellectual» attack.**

Ключевые слова: **Парольная защита, безопасность пароля, силовой перебор паролей, «интеллектуальный» взлом.**

I Введение

Механизмы парольной защиты (ПЗ) широко используются в компьютерных технологиях в целях предотвращения несанкционированного доступа (НСД) при загрузке операционной системы, открытии различных приложений, доступе к информационным ресурсам, входе в компьютерные сети и др. Поэтому оценка надежности ПЗ и разработка практических рекомендаций по ее усилению являются актуальными задачами [1 – 4]. В немалой степени этому способствует и постоянное совершенствование аппаратно-программного обеспечения и технологий для взлома парольной защиты [5 – 7].

В общем случае вероятность *P* подбора пароля злоумышленником описывается функцией [2]:

$$P = F(m, n, P_1, s(t), T), \qquad (1)$$

где: *m* – размер алфавита, из символов которого может быть составлен пароль;

n – длина пароля (количество символов в пароле);
P_1 – вероятность подбора пароля с одной попытки;
$s(t)$ – количество возможных попыток за единицу времени;
T – интервал времени, в течение которого осуществляется взлом.

Известны частные конкретизации (1) для различных случаев. Например, формула Андерсона [1], позволяющая оценить вероятность подбора пароля удаленным злоумышленником при фиксированных скорости передачи символов в линии связи, числе символов в каждом передаваемом сообщении, времени взлома, размере алфавита и длине пароля.

II Постановка задачи

Представляется актуальной постановка и решение (1) для другого частного случая: нахождения времени безопасной работы Ts при заданных: размере алфавита m, длине пароля n и времени проверки одного варианта пароля t_1. Данная ситуация возникает, когда время НСД и количество попыток взлома практически не ограничены, алгоритм взлома основан на применении метода “грубой силы” (brute force) – переборе всех возможных и равновероятных символов в пароле при ограниченном быстродействии компьютера злоумышленника.

Также представляет практический интерес анализ полученных результатов для случая неравновероятных вариантов использования символов в пароле при заданных параметрах m,n,t_1.

III Оценка безопасности парольной защиты при взломе силовым методом

Время, необходимое для перебора всех возможных вариантов пароля и называемое временем безопасности пароля, определяется выражением [3]:

$$T_s = \sum_{i=1}^{n} m^i \cdot t_1 . \qquad (2)$$

Выражение (2) можно записать в виде:

$$T_s = \sum_{i=1}^{n-1} m^i \cdot t_1 + m^n \cdot t_1 \text{ или } T_s = S_{n-1} \cdot t_1 + m^n \cdot t_1 , \qquad (3)$$

где: $S_{n-1} = \sum_{i=1}^{n-1} m^i$ – сумма первых (n-1) слагаемых выражения (2).

В выражении (3) слагаемым, в значительной степени определяющим время безопасности T_s, является $m^n * t_1$. Остальные же слагаемые добавляют в сумме не более 10% при размере алфавита m=10 символов. При этом вклад S_{n-1} в общую сумму уменьшается при увеличении m. На рис. 1 по оси абсцисс указана длина пароля n, а по оси ординат – погрешность вычисления времени безопасности пароля: δ – вклад в процентном соотношении первых (n–1) слагаемых выражения (3) в общую сумму. Кривые построены для различных значений размера алфавита m.

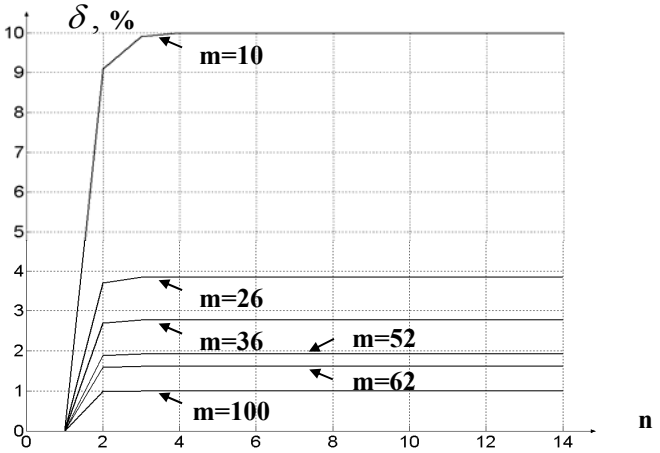


Рисунок 1 – К расчету погрешности вычислений

Отсюда видно, что для приближенной оценки необходимого времени безопасности пароля можно воспользоваться формулой

$$T_s = m^n \cdot t_1 . \tag{4}$$

Тогда длина пароля, необходимая для обеспечения заданного времени безопасности, будет определяться выражением

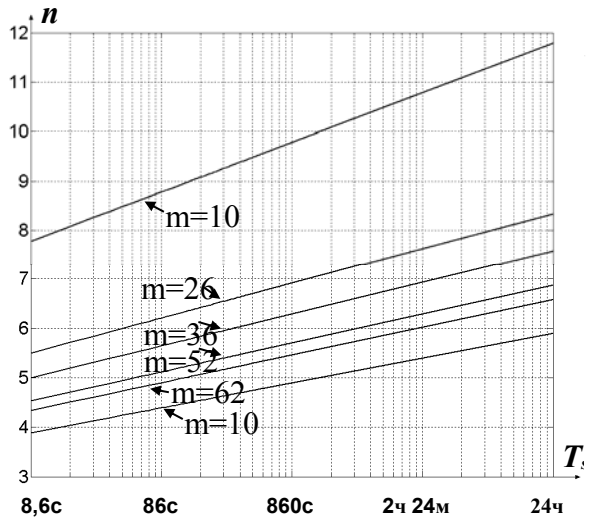
$$n \geq \log_m \frac{T_s}{t_1} . \tag{5}$$

Так, например, при T_s=100 дней, m=26 символов и t_1=0,001 сек, $n \geq 7{,}0224$. Таким образом, минимальная длина n, обеспечивающая заданное время безопасности пароля, может быть получена при округлении расчетного по (5) значения n до ближайшего большего целого (n=8).

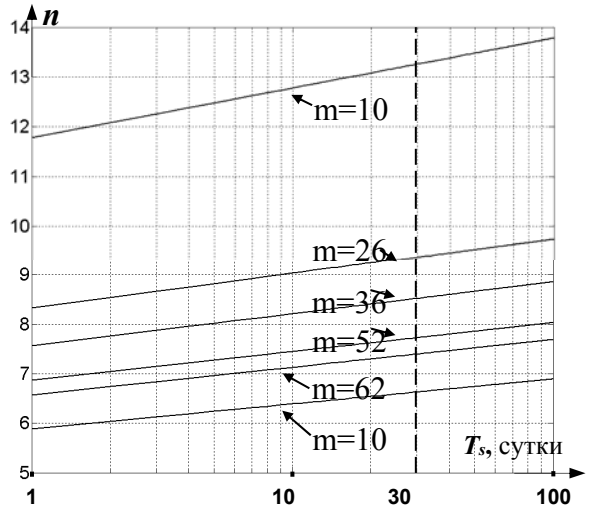
На графиках (рис. 2) приведены зависимости длины пароля n от требуемого времени безопасности T_s для разных размеров алфавита m. За основу расчетов взята одна из программ подбора пароля на вход в операционную систему Windows XP. Максимальная скорость работы данной версии программы на компьютере с процессором Intel Celeron 2,66 ГГц составила 7 млн. паролей в секунду (t_1=1,43·10^{-7}сек).

Анализ приведенных на рис. 2 зависимостей показывает, что при выборе пароля необходимо стремиться к увеличению размера m и количества символов в пароле n. Это возможно при:

- использовании всех букв, цифр и специальных символов стандартной клавиатуры (с верхним и нижним регистром);
- использовании специальных символов, отсутствующих на клавиатуре, но доступных посредством набора их кода на дополнительном цифровом поле стандартной клавиатуры (при нажатой клавише Alt);
- установке минимальной длины пароля n, соответствующей требуемому значению T_s в соответствии с выражением (5);
- периодической смене пароля через время $T \leq T_s$.



а)



б)

Рисунок 2 – Оценка времени безопасности ПЗ

IV Оценка безопасности парольной защиты при взломе “интеллектуальным” методом защиты

В [3, 8] отмечалось, что около 80% всех паролей, содержащих 8 символов и более, успешно подбиралось на основе методов “интеллектуального” взлома. Последние могут быть основаны на знании отдельных символов пароля (переборе по маске), наличии априорных сведений о пользователе (социальной инженерии), применении тезаурусов наиболее употребительных слов и словосочетаний, учете устойчивых языковых особенностей и других, зачастую эвристически выбираемых параметрах.

Ниже рассматривается задача оценки безопасности парольной защиты для случая использования злоумышленником, например, известных и неравномерных законов распределения частоты языковых символов в осмысленных словосочетаниях для различных алфавитов.

Формула Андерсона [1], приведенная в СИ, имеет вид

$$\frac{T}{t_1 P} \le m^n \text{ или } T \le T_s P \,. \qquad (6)$$

Здесь: $T_s=m^n \times t_1$ – время, необходимое для полного перебора всех возможных символов в пароле, или время безопасной работы; T - время (в секундах), в течение которого могут быть предприняты систематические попытки подбора пароля; P – вероятность того, что пароль может быть раскрыт за указанное время.

Таким образом, из (6) следует, что для P=1 необходимо обеспечить перебор всех возможных вариантов пароля (при этом $T=Ts$). С вероятностью 50% пароль может быть найден, если перебрать половину вариантов из множества m^n и т. д.

На графике (рис. 3) пунктирной линией показана зависимость (6) между временем, затрачиваемым на взлом T, и длиной пароля n, вычисленная для P=0,5, m=26 (английский алфавит, малые строчные буквы), которая была исследована ранее при P=1 и различных размерах алфавита m.

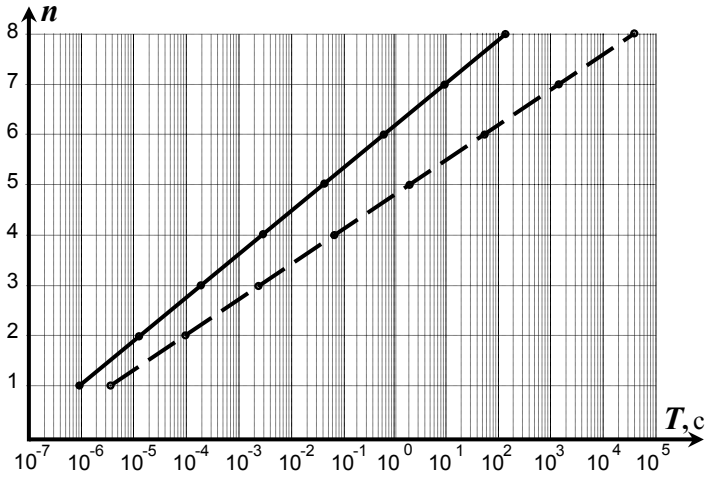


Рисунок 3 – Выигрыш во времени при «интеллектуальном» взломе

Однако, если символы в пароле не равновероятны, то методом “интеллектуального” взлома возможен перебор в порядке, например, убывания их вероятности, что может позволить существенно сократить время подбора пароля по сравнению с силовым методом (при заданных P, m, n).

На рис. 4 показаны двумерные плотности вероятности пароля $P_{пароля}$, составленного из двух символов русского (а) и английского языков (б), используемые при моделировании. Здесь же приведены сечения указанных двумерных плотностей плоскостями, параллельными координатным осям, которые отображают известные вероятности появления символов $P_{символов}$ в осмысленных словосочетаниях русского (в) и английского (г) языков [9].

Сплошной линией на рис. 3 показана зависимость требуемой длины пароля n от времени T, которое может быть затрачено на его взлом, при учете указанных статистических зависимостей по данным моделирования (P=0,5; m=26, английский алфавит, малые строчные буквы).

Анализ полученных результатов позволяет сделать вывод, что учет частоты появления символов при “интеллектуальном” взломе позволяет примерно на порядок уменьшить требуемое время перебора, начиная с длины пароля n=3 символа. При дальнейшем увеличении длины пароля n указанный выигрыш возрастает примерно на порядок для каждого последующего увеличения длины пароля на 3 символа. Аналогичные результаты получены и для русского алфавита.

Таким образом, учет частоты появления символов при “интеллектуальном” взломе паролей, представляющих осмысленные словосочетания, позволяет существенно сократить требуемое время перебора, или, что эквивалентно, уменьшить время безопасности пароля на несколько порядков.

Еще больший временной выигрыш в подборе осмысленных паролей может дать их перебор по специальным словарям, которые представляют собой заранее сформированный список слов, наиболее часто используемых на практике в качестве паролей [7]. К каждому слову из словаря парольный взломщик

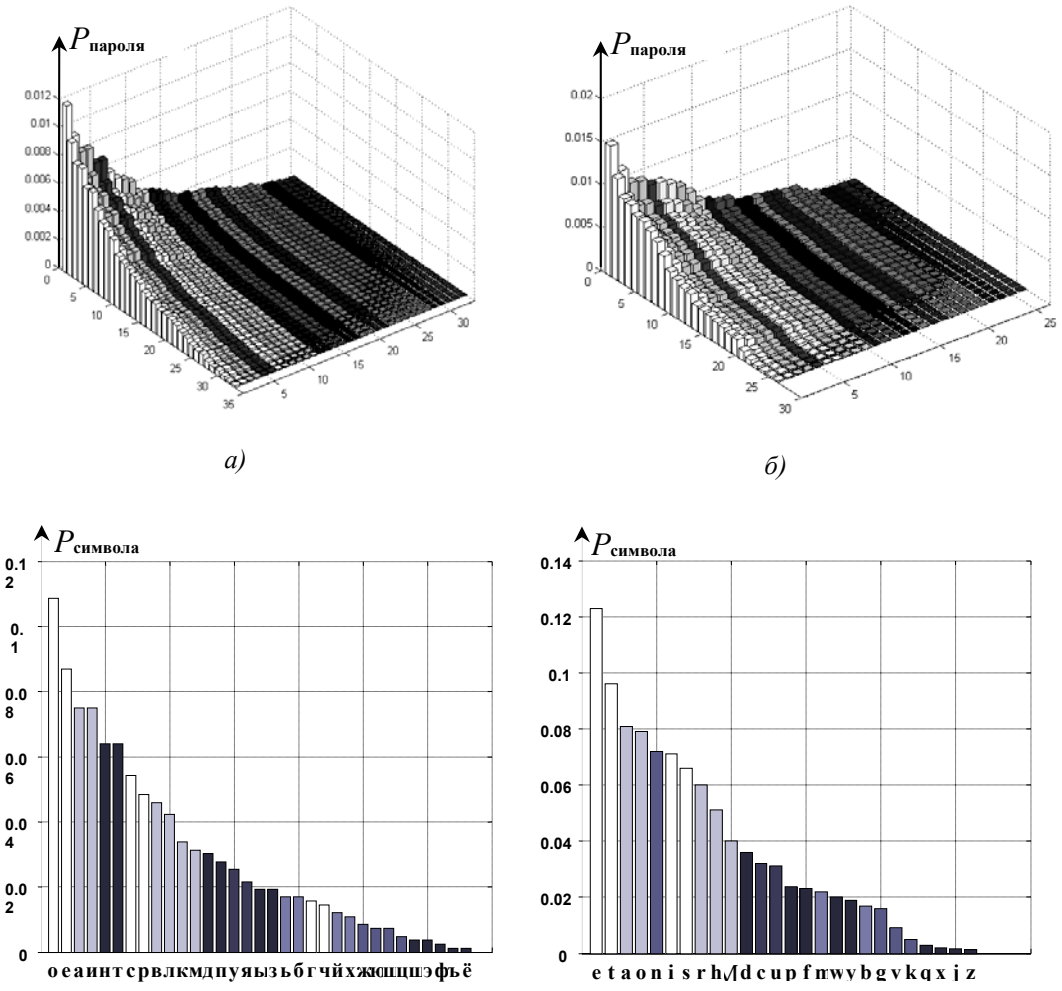
применяет одно или несколько правил, в соответствии с которыми оно видоизменяется и порождает дополнительное множество опробуемых паролей, например:

- попеременное изменение буквенного регистра, в котором набрано слово;
- изменение порядка следования букв в слове на обратный;
- приписывание в начало и в конец каждого слова цифр;
- транслитерация русских букв латинскими;
- изменение некоторых букв на близкие по начертанию цифры;
- замена раскладок клавиатуры;
- запись слова без гласных за исключением заглавной буквы и др.

Преимущество такого метода “интеллектуального” взлома – его высокая скорость.

Недостатком является возможность нахождения только очень простых паролей, которые имеются в словаре в прямом или модифицированном виде. Успех реализации данной атаки напрямую зависит от качества и объема используемых словарей.

Таким образом, кроме вышеизложенных рекомендаций по выбору пароля, следует обеспечить также статистическую независимость между символами в нем и отсутствие подобных словосочетаний в известных тезаурусах. Это может достигаться, например, генерацией случайных парольных символов с помощью специальных программ. Одна из таких программ – *Advanced Password Generator* позволяет создавать пароли с помощью генератора случайных чисел либо по задаваемому пользователем ключевому слову, а также содержит алгоритм создания слов, наиболее близких к естественному языку (русскому или английскому). При использовании указанного режима получаются “запоминаемые”, но не имеющие смысла слова.



а) *б)*

в) *г)*

Рисунок 4 – Моделирование статистических зависимостей между символами в пароле

Дальнейшее увеличение эффективности ПЗ может достигаться за счет:

- установления минимальной длины пароля (не менее 8 символов из букв, цифр, специальных знаков в двух регистрах);
- установления максимального срока действия пароля (до 1 месяца);
- обеспечения невозможности замены пароля по истечении его срока действия на один из используемых ранее;
- ограничения числа попыток неправильного ввода пароля;
- обеспечения замкнутости программной среды и др.

V Выводы

Безопасность ПЗ в современных программных продуктах в значительной степени зависит от качества произвольно выбираемых пользователем (администратором) или генерируемых автоматически паролей.

Изложенные выше оценки и рекомендации позволяют повысить безопасность ПЗ для методов взлома, основанных на силовом переборе возможных равновероятных вариантов, на использовании известных вероятностей появления символов в осмысленных словосочетаниях, а также частотных словарей вероятных паролей.

При этом кардинальными методами усиления ПЗ являются введение ограничений на число неверно введенных значений пароля и обеспечение замкнутости программной среды, не позволяющей злоумышленнику запустить программы – парольные взломщики. Однако их практическая реализация в ряде случаев затруднена.

Литература: ***1.*** *Хофман Л. Дж. Современные методы защиты информации. М.: Советское радио, 1980.* ***2.*** *Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и техника, 2004.* ***3.*** *Анин Б. Ю. Защита компьютерной информации.– СПб: БХВ–Петербург, 2000.* ***4.*** *Емельянов С. Л., Гаращук В. В. Некоторые аспекты безопасности парольной защиты//Вісник ЧДТУ, №2/2006, С. 155–157.* ***5.*** *Безмалый В. Ф. Краткий обзор программ-взломщиков паролей//http:// www.zahist.kiev.ua. .****6.*** *Г. Красноступ, Д. Кудин. Шпионские программы и новейшие методы защиты от них // Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", Вип..9, 2004, С. 67–75.* ***7.*** *В. Безмалый. Чем нас пытаются взломать // www.itacademy.com.ua .****8.*** *http://www.bezpeka.com–Официальный сайт "Центра информационной безопасности".****9.*** *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях./Под ред. В. Ф. Шаньгина . – М.: Радио и связь, 1999.*

УДК 681.3

АНТИВІРУСНІ ПРОГРАМИ СВІТОВИХ БРЕНДІВ: ПОРІВНЯЛЬНА ОЦІНКА МОЖЛИВОСТЕЙ, РЕКОМЕНДАЦІЇ З ЇХ ВИБОРУ, НОВИЙ МЕТОД ПРОГНОЗУВАННЯ АНТИВІРУСНОЇ БЕЗПЕКИ

Вячеслав Шорошев
ДНДІ МВС України

Аннотация: **Надаються порівняльна оцінка світових лідерів антивірусних програм, рекомендації по їх вибору, а також метод прогнозування антивірусної безпеки в комп'ютерних системах і мережах.**
Summary: **The guidelines on their selection, and also method of forecasting (prediction) of anti-virus safety are given a comparative estimation of the world (global) leaders of the anti-virus programs.**
Ключові слова: **Антивірусні програми, детектуваня вірусів, виявлення вірусів, розпізнавання вірусів, антивірусна безпека, ризик антивірусної безпеки.**

I Вступ

Рейтингові оцінки антивірусних програм світових брендів і зростання їх можливостей в останній час досить вагомі. Але одних рейтингових оцінок антивірусних програм вже недостатньо. Для адміністратора безпеки завжди важливо знати – по-перше, який комплект антивірусних програм найбільш пріоритетний для підвищення антивірусної безпеки оцінюваної комп'ютерної системи або локальної мережі, особливо