ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

ЗАЩИТА ИНФОРМАЦИИ

INFORMATION PROTECTION

УДК 004
https://doi.org/10.37661/1816-0301-2020-17-3-64-71

Поступила в редакцию 04.05.2020
Received 04.05.2020

Принята к публикации 14.07.2020
Accepted 14.07.2020

Стойкость механизмов аутентификации в инфокоммуникационных сетях

М. Н. Бобов✉, А. В. Курилович

Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь
✉E-mail: bobov@bsuir.by

Аннотация. Рассмотрены распределенные инфокоммуникационные сети, в которых осуществляется взаимодействие пользователей, серверов приложений и баз данных для обеспечения реализации различных прикладных задач. При доступе к инфокоммуникационной сети первой процедурой является установление подлинности взаимодействующих субъектов посредством их аутентификации на основе использования механизма паролей. Показано, что для социальных сетей с большим числом пользователей широко применяемая оценка безопасности парольных систем на основе расчета вероятности его подбора недостаточна. Приведены графики вероятности появления одинаковых паролей у двух пользователей при длине пароля 6, 7 и 8 знаков, объеме алфавита 36, 42 и 57 знаков и количестве пользователей не более 10^7. Дана оценка стойкости парольных систем аутентификации инфокоммуникационных сетей на основе критерия «парадокс дней рождения». Определено, что известные социальные сети, имеющие число пользователей, сравнимое с числом используемых паролей, являются нестойкими к атакам «дней рождения». Показано, что для таких систем стойкость парольной системы к взлому должна оцениваться исходя из критерия $m = A^{n/2}$.

Ключевые слова: аутентификация, стойкость парольной системы, инфокоммуникационная сеть, удаленный доступ, парадокс дней рождения, критерий стойкости сети к атакам «дней рождения»

Для цитирования. Бобов, М. Н. Стойкость механизмов аутентификации в инфокоммуникационных сетях / М. Н. Бобов, А. В. Курилович // Информатика. – 2020. − Т. 17, № 3. – С. 64–71. https://doi.org/10.37661/1816-0301-2020-17-3-64-71

Stability of password authentication in infocommunication networks

Mikhail N. Bobov✉, Andrei V. Kurylovich

Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus
✉E-mail: bobov@bsuir.by

Abstract. The article discusses distributed infocommunication networks, in which the interaction of users, application servers and databases is carried out. When accessing an infocommunication network, the first procedure is to authenticate the agents through their authentication by password mechanism. It is shown that for social networks with a large number of users, widely used assessment of the security of password systems based on the calculation of the determination probability is not sufficient. The probability of the same passwords for two users with a password length of 6, 7 and 8 characters with alphabet size of 36, 42 and 57 characters and the number of users no more than 10 million is shown. An assessment of the strength of password authentication

systems for info-communication networks based on the "birthday paradox" criterion is given. It has been determined that well-known social networks with a number of users comparable to the number of passwords used are not resistant to "birthday attacks". It is shown that for such systems the resistance of the password system to cracking should be assessed by $m = A^{n/2}$ criterion.

Keywords: password authentication, password system stability, infocommunication networks, remote access, the "birthday paradox", networks strength criteria of password authentication

For citation. Bobov M. N., Kurylovich A. V. Stability of password authentication in infocommunication networks. *Informatics*, 2020, vol. 17, no. 3, pp. 64−71 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-3-64-71

Введение. Целью функционирования инфокоммуникационных сетей является реализация информационных процессов с заданными характеристиками, направленных на обеспечение различных прикладных задач пользователей. Для их решения в системе осуществляются взаимодействия пользователей между собой, пользователей с серверами приложений и баз данных, между серверами приложений и баз данных. Краеугольным вопросом при организации таких взаимодействий является установление подлинности субъектов, пытающихся получить доступ к ресурсам системы. Данная проблема решается путем использования средств и методов аутентификации, которые по месту приложения можно разделить на локальные и удаленные. При локальной аутентификации вся система, включая механизм аутентификации и управления доступом, размещается внутри одного физического периметра безопасности. Владелец системы и (или) пользователь ведут и обновляют базу аутентификационных данных внутри этого периметра. Аутентификация предполагает непосредственное взаимодействие субъекта с устройством проверки подлинности при входе в систему.

Удаленная аутентификация используется при взаимодействии пользователей с информационными ресурсами сети или другими пользователями в интерактивном режиме, содержит несколько точек обслуживания, которые требуют управления доступом и могут размещаться в различных местах. Владелец ведет и поддерживает актуальной единую базу аутентификационных данных для всей системы [1].

В настоящее время широкое распространение получили распределенные информационные сети, созданные для обеспечения потребностей широкого круга пользователей и имеющие условное наименование «социальные сети». Каждый пользователь для получения доступа к подобной сети на первом этапе проходит процедуру регистрации, в процессе которой сообщает системе свои учетное имя и пароль, а также другие персональные данные. В дальнейшем при обращении к сети для получения ее услуг пользователь вводит учетное имя и пароль и при их совпадении с именем и паролем, введенными при регистрации, получает доступ к сети.

Являясь средствами защиты каналов доступа к инфокоммуникационным системам, механизмы аутентификации должны обладать рядом специфических качеств, обеспечивающих их стойкость к взлому, который может происходить путем подбора пароля, компрометации пароля или кражи файла паролей. Вероятность подбора пароля зависит в основном от двух параметров: длины пароля и объема алфавита, и если пароль выбирается случайно и равновероятно, то для ее оценки используются формулы, широко применяемые для локальных парольных механизмов [2]:

– вероятность подбора пароля с первой попытки

$$P_{П1} = \frac{1}{A^S},$$

где A – объем алфавита, S – длина пароля;

– вероятность подбора пароля с i-й попытки

$$P_{П1} = \frac{1}{A^S + 1 - i};$$

– вероятность подбора пароля за k попыток

$$P_{Пk} = \frac{k}{A^S};$$

– вероятность подбора пароля в период его безопасного времени действия

$$P_{\text{Т}_\text{Б}} = \frac{3600 \cdot T_\text{Б}}{A^S \cdot t_\text{П}},$$

где $T_\text{Б}$ – безопасное время действия; $t_\text{П}$ – время набора пароля.

Вместе с тем широко известные современные социальные сети объединяют огромное количество пользователей, и поэтому оценки стойкости используемых в них парольных систем аутентификации к атакам подбора пароля, компрометации пароля и краже файла паролей недостаточно. В рассматриваемом случае парольные системы аутентификации необходимо оценивать на стойкость к атакам «дней рождения». Атака «дней рождения» – используемое в криптоанализе название для метода взлома шифров или поиска коллизий хеш-функций на основе парадокса дней рождения [3]. Парадокс дней рождения – положение, утверждающее, что если дана группа из 23 или более человек, то вероятность того, что хотя бы у двух из них дни рождения (число и месяц) совпадут, превышает 50 %. Для группы из 60 или более человек вероятность совпадения дней рождения хотя бы у двух ее членов составляет более 99 %, хотя 100 % она достигает, только когда в группе находится не менее 367 человек (с учетом високосных лет).

Определим вид формального выражения для расчета вероятности совпадения хотя бы двух паролей размерности n в группе из m пользователей. Рассчитаем сначала вероятность $p(m)$ того, что в группе из m пользователей все их пароли будут различными. Если $N > m$ ($N = A^n$), то в силу принципа Дирихле вероятность равна нулю. Если же $N \le m$, то будем рассуждать следующим образом. Возьмем наугад одного пользователя из группы и запомним его пароль. Затем возьмем наугад второго пользователя, при этом вероятность того, что его пароль не совпадет с паролем первого пользователя, равна $1 - 1/N$. После этого возьмем третьего пользователя, при этом вероятность того, что его пароль не совпадет с паролями первых двух, равна $1 - 2/N$. Рассуждая по аналогии, дойдем до последнего пользователя, для которого вероятность несовпадения его пароля со всеми предыдущими будет равна $1 - (m-1)/N$. Перемножая эти вероятности, получим вероятность того, что все пароли в группе будут различными:

$$\begin{aligned} p(m) &= 1 \cdot (1 - 1/N) \cdot (1 - 2/N) \cdot \ldots \cdot (1 - (m-1)/N) = \\ &= \frac{N \cdot (N-1) \cdot \ldots \cdot (N-m+1)}{N^m} = \frac{N!}{(N-m)! \cdot N^m}. \end{aligned} \tag{1}$$

Тогда вероятность того, что по крайней мере один пользователь имеет тот же пароль, что и любой другой пользователь из группы m, определяется выражением

$$P(m) = 1 - \frac{N!}{(N-m)! \cdot N^m}. \tag{2}$$

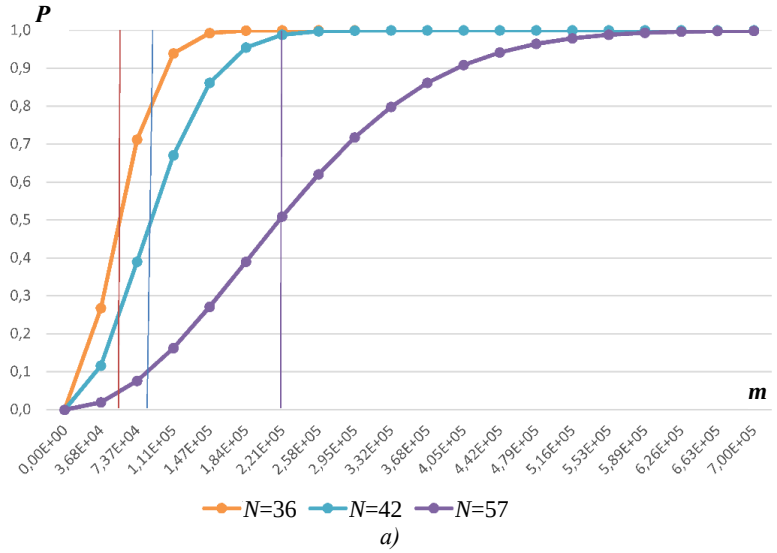
Воспользуемся формулой Стирлинга для приближенного вычисления значения факториала $n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ для расчета полученной функции:

$$\begin{aligned} P(m) = 1 - \frac{N!}{(N-m)! \cdot N^m} &\approx 1 - \frac{\sqrt{2\pi N}\left(\frac{N}{e}\right)^N}{N^m \cdot \sqrt{2\pi(N-m)}\left(\frac{N-m}{e}\right)^{(N-m)}} = \\ &= 1 - \sqrt{\frac{N}{N-m}} \cdot \frac{1}{e^m} \cdot \left(\frac{N}{N-m}\right)^{(N-m)}. \end{aligned}$$

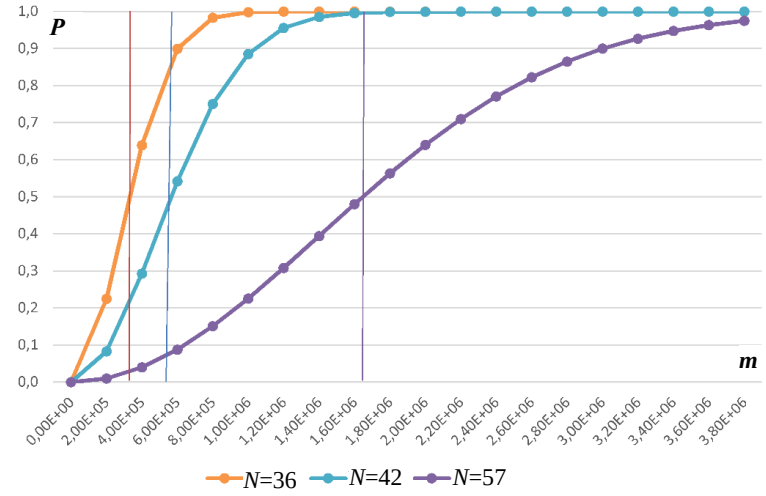
Таким образом, получим формулу

$$P(m) \approx 1 - \sqrt{\frac{N}{N-m}} \cdot \frac{1}{e^m} \cdot \left(\frac{N}{N-m}\right)^{(N-m)}. \tag{3}$$

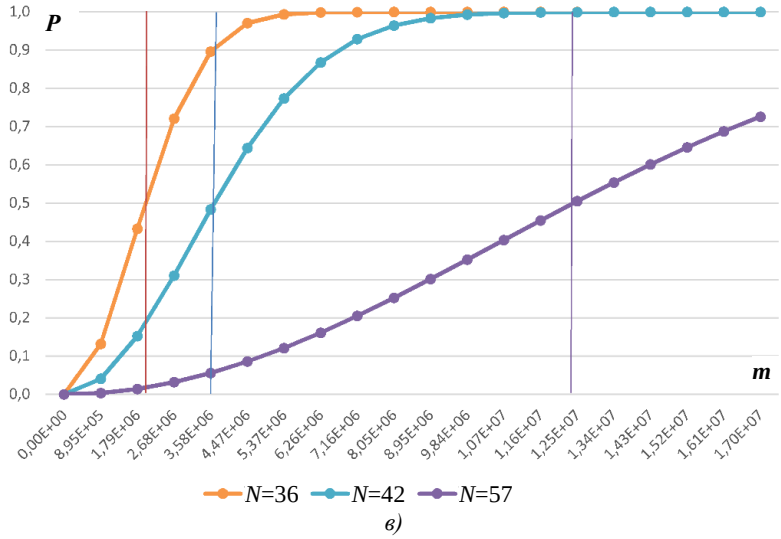
На рис. 1 изображены графики вероятности появления одинаковых паролей у двух пользователей из предположения, что пароли выбираются случайно и равновероятно. Расчет выполнен в программе Mathematica для следующих исходных условий: количество знаков в алфавите $N = 36, 42, 57$; длина пароля $n = 6, 7, 8$; количество пользователей $m = 1 – 1{,}7 \cdot 10^7$.



а)



б)



в)

Рис. 1. Графики вероятности $P(m)$ при длине пароля n = 6 (*а*); n = 7 (*б*) и n = 8 (*в*)

По отношению к атаке «дней рождения» сформулируем следующий критерий стойкости парольной системы аутентификации. Парольная система аутентификации считается стойкой, если величина вероятности совпадения двух назначаемых в ней паролей меньше 0,5, т. е. верно неравенство

$$P(m) < 0{,}5. \tag{4}$$

Другими словами, парольная система аутентификации считается нестойкой, если величина вероятности совпадения двух назначаемых в ней паролей $P(m) \geq 0{,}5$. Данные о количестве пользователей, соответствующем принятому критерию (на рис. 1 отмечены вертикальными линиями), приведены в табл. 1.

Таблица 1

Размер алфавита	$P(m) = 0{,}5$			$P(m) = 0{,}9$		
	$n = 6$	$n = 7$	$n = 8$	$n = 6$	$n = 7$	$n = 8$
36	$3{,}7 \cdot 10^4$	$4{,}0 \cdot 10^5$	$1{,}8 \cdot 10^6$	$1{,}1 \cdot 10^5$	$6{,}0 \cdot 10^5$	$3{,}5 \cdot 10^6$
42	$9{,}5 \cdot 10^4$	$6{,}0 \cdot 10^5$	$3{,}5 \cdot 10^6$	$1{,}8 \cdot 10^5$	$1{,}2 \cdot 10^6$	$7{,}2 \cdot 10^6$
57	$2{,}2 \cdot 10^5$	$1{,}6 \cdot 10^6$	$1{,}3 \cdot 10^7$	$4{,}0 \cdot 10^5$	$3{,}0 \cdot 10^6$	$\sim 10^9$

Для указанных параметров системы с числом пользователей, расположенным слева от прямых на рис. 1, являются нестойкими. В качестве примера оценим стойкость наиболее распространенных социальных сетей, сведения по которым приводятся в исследовании компании WebCanape, проведенном в январе 2019 г. (рис. 2) (URL: https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii).

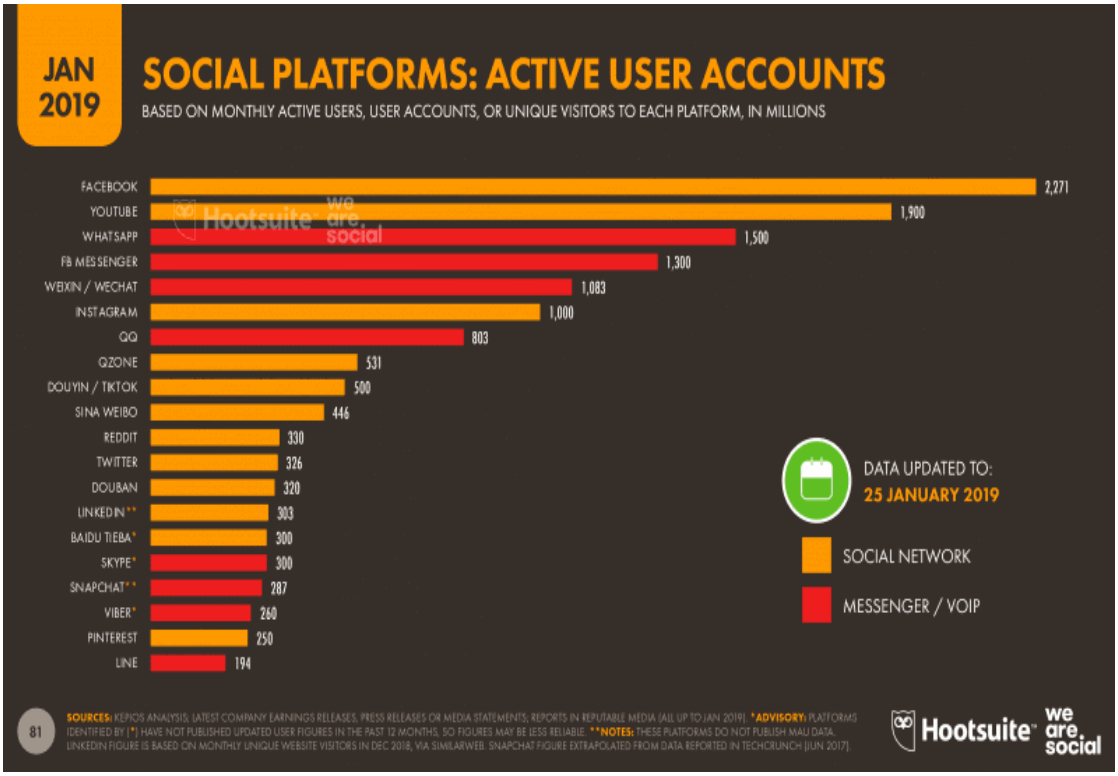


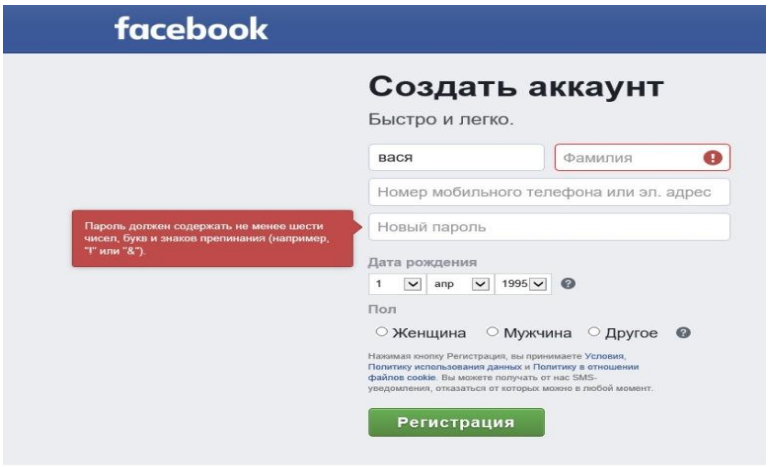
Рис. 2. Данные о количестве пользователей, зарегистрированных в наиболее популярных сетях

Количество учетных записей пользователей наиболее распространенных социальных сетей приведено в табл. 2.

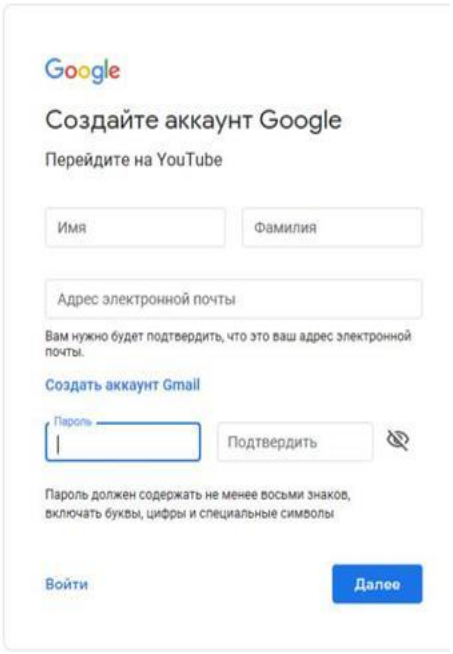
Таблица 2

Сеть	Количество пользователей
Facebook	2,27 млрд ($2{,}27\cdot10^9$)
YouTube	1,9 млрд ($1{,}9\cdot10^9$)
Instagram	1,0 млрд ($1{,}0\cdot10^9$)
Ozone	536 млн ($5{,}31\cdot10^8$)
Twitter	326 млн ($3{,}26\cdot10^8$)
LinkedIn	303 млн ($3{,}03\cdot10^8$)

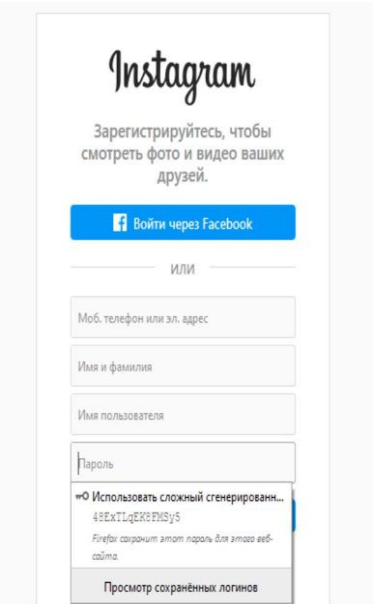
При регистрации социальные сети предъявляют к паролям различные требования (рис. 3).



а)



б)



в)

Рис. 3. Регистрация в Facebook (*а*); YouTube (*б*) и Instagram (*в*)

Минимально необходимые параметры парольных систем аутентификации, используемые в распространенных социальных сетях, представлены в табл. 3.

Таблица 3

Сеть	Количество пользователей	Алфавит A	Длина пароля n	$P_{П1}$
Facebook	$2{,}27\cdot10^9$	42	6	$5{,}5\cdot10^9$
YouTube	$1{,}9\cdot10^9$	42	8	$9{,}6\cdot10^{12}$
Instagram	$1{,}0\cdot10^9$	62	15	$4{,}8\cdot10^{28}$
Ozone	$5{,}31\cdot10^8$	36	6	$2{,}1\cdot10^9$
Twitter	$3{,}26\cdot10^8$	36	6	$2{,}1\cdot10^9$
LinkedIn	$3{,}03\cdot10^8$	36	6	$2{,}1\cdot10^9$

Сравнительные данные по существующему и допустимому числу пользователей в анализируемых социальных сетях, использующих парольные системы аутентификации с указанными при регистрации параметрами, в соответствии с критерием стойкости к атаке «дней рождения» приведены в табл. 4.

Таблица 4

Сеть	Количество пользователей	Количество пользователей по критерию $P(m) = 0{,}5$	$P_{П1}$	Оценка
Facebook	$2{,}27\cdot10^9$	$9{,}5\cdot10^4$	$5{,}5\cdot10^9$	–
YouTube	$1{,}9\cdot10^9$	$3{,}6\cdot10^6$	$9{,}6\cdot10^{12}$	–
Instagram	$1{,}0\cdot10^9$	$\sim10^{12}$	$4{,}8\cdot10^{28}$	Соответствует
Ozone	$5{,}31\cdot10^8$	$3{,}7\cdot10^4$	$2{,}1\cdot10^9$	–
Twitter	$3{,}26\cdot10^8$	$3{,}7\cdot10^4$	$2{,}1\cdot10^9$	–
LinkedIn	$3{,}03\cdot10^8$	$3{,}7\cdot10^4$	$2{,}1\cdot10^9$	–

Как следует из данных табл. 4, среди анализируемых социальных сетей только Instagram является стойкой к атаке «дней рождения».

Определим теперь аналитическое выражение для практического расчета стойкости сети к атаке «дней рождения» [4]. Используя выражение (1), найдем показатель

$$P(m) = 1 - 1\cdot(1 - 1/N)\cdot(1 - 2/N)\cdot, \ldots, \cdot(1 - (m-1)/N) =$$

$$= 1 - \prod_{i=1}^{m-1}\left(1 - \frac{i}{N}\right) \approx 1 - \prod_{i=1}^{m-1}\left(e^{-\frac{i}{N}}\right) = 1 - e^{-\frac{m(m-1)}{N}}.$$

Согласно критерию (4)

$$1 - e^{-\frac{m(m-1)}{N}} = \frac{1}{2},\ 2 = e^{\frac{m(m-1)}{2\cdot N}},\ ln2 = \frac{m(m-1)}{2\cdot N}.$$

Принимая $m(m-1) \approx m^2$, получим выражение

$$m = \sqrt{2N\cdot ln2} = 1{,}17\sqrt{N} = \sqrt{A^n} = A^{\frac{n}{2}}.$$

Таким образом, парольные системы аутентификации, применяемые в больших распределенных сетях, в которых число пользователей m сравнимо или больше возможного количества вы-

бираемых ими для доступа к услугам аутентификаторов N, должны оцениваться на стойкость к атаке «дней рождения» в соответствии с критерием $m = A^{n/2}$.

Список использованных источников

1. Бобов, М. Н. Основы аутентификации в телекоммуникационных системах : учеб. пособие / М. Н. Бобов, В. К. Конопелько. – Минск : БГУИР, 2008. – 130 с.

2. Смит, Р. Э. Аутентификация: от паролей до открытых ключей : пер. с англ. / Р. Э. Смит. – М. : Вильямс, 2002. – 432 с.

3. Математические и компьютерные основы криптологии / Ю. С. Харин [и др.]. – Минск : Новое знание, 2003. – 382 с.

4. Мао, В. Современная криптография: теория и практика : пер. с англ. / В. Мао. – М. : Вильямс, 2005. – 768 с.

References

1. Bobov M. N., Konopelko V. K. Osnovy autentifikatsii v telekommunikatsionnykh sistemakh. *Basics of Authentication in Telecommunication Systems*. Minsk, Belorusskij gosudarstvennyj universitet informatiki i radiojelektroniki, 2008, 130 p. (in Russian).

2. Smith R. E. *Authentication: from Passwords to Public Keys*. Boston, Addison Wesley, 2002, 549 p.

3. Kharin Y. S., Bernik V. I., Matveyev G. V., Agiyevich S. V. Matematicheskiye i komp'yuternyye osnovy kriptologii. *Mathematical and Computer Foundations of Cryptology*. Minsk, Novoye znaniye, 2003, 382 p. (in Russian).

4. Mao W. *Modern Cryptography: Theory and Practice*. New Jersey, Prentice Hall PTR, 2003, 648 p.

Информация об авторах

Бобов Михаил Никитич, доктор технических наук, профессор, Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь.
E-mail: bobov@bsuir.by

Курилович Андрей Владимирович, старший преподаватель кафедры инфокоммуникационных технологий, Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь.
E-mail: kurilovich@bsuir.by

Information about the authors

Mikhail N. Bobov, Dr. Sci. (Eng.), Professor, Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus.
E-mail: bobov@bsuir.by

Andrei V. Kurylovich, Senior Lecturer of the Department of Infocommunication Technologies, Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus.
E-mail: kurilovich@bsuir.by