Стойкость механизмов аутентификации в инфокоммуникационных сетях

Автор доклада

Бобов М.Н., д.т.н., профессор

УО «Белорусский государственный университет информатики и радиоэлектроники» г. Минск

Стойкость механизмов аутентификации в инфокоммуникационных сетях

В настоящее время широкое распространение получили распределённые информационные сети, созданные для обеспечения потребностей широкого круга пользователей и имеющие условное наименование «социальные сети».

Каждый пользователь для получения доступа к такой сети на первом этапе проходит процедуру регистрации, в процессе которой сообщает системе своё учётное имя и пароль, а также другие учётные персональные данные.

Как средства защиты каналов доступа к инфокоммуникационным системам, механизмы аутентификации должны обладать рядом специфических качеств, обеспечивающих их стойкость к взлому.

Для оценки стойкости используются формулы, широко применяемые для локальных парольных механизмов:

Стойкость механизмов аутентификации в инфокоммуникационных сетях

Вероятность подбора пароля с первой попытки:

$$P_{П1} = \frac{1}{A^S},$$

где: A – объём алфавита; S – длина пароля.

Вероятность подбора пароля с i – ой 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:

$$P_{Т_Б} = \frac{3600 \cdot Т_Б}{A^S \cdot t_П},$$

где $Т_Б$ – безопасное время действия; $t_П$ – время набора пароля.

Стойкость механизмов аутентификации в инфокоммуникационных сетях

Широко известные современные социальные сети объединяют огромное количество пользователей, поэтому оценку стойкости используемых в них парольных систем аутентификации необходимо оценивать на стойкость к атакам «день рождения».

Атака «дней рождения» – используемое в криптоанализе название для метода взлома шифров или поиска коллизий хеш-функций на основе парадокса дней рождения.

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 примера у группы из 60 или более человек, вероятность совпадения дней рождения хотя бы у двух её членов составляет более 99%.

Фрмальное выражение для расчёта вероятности совпадения хотя бы двух паролей размерности n в группе из m пользователей имеет вид;

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

Стойкость механизмов аутентификации в инфокоммуникационных сетях

Ниже приведены 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 A $= 36, 42, 57$;

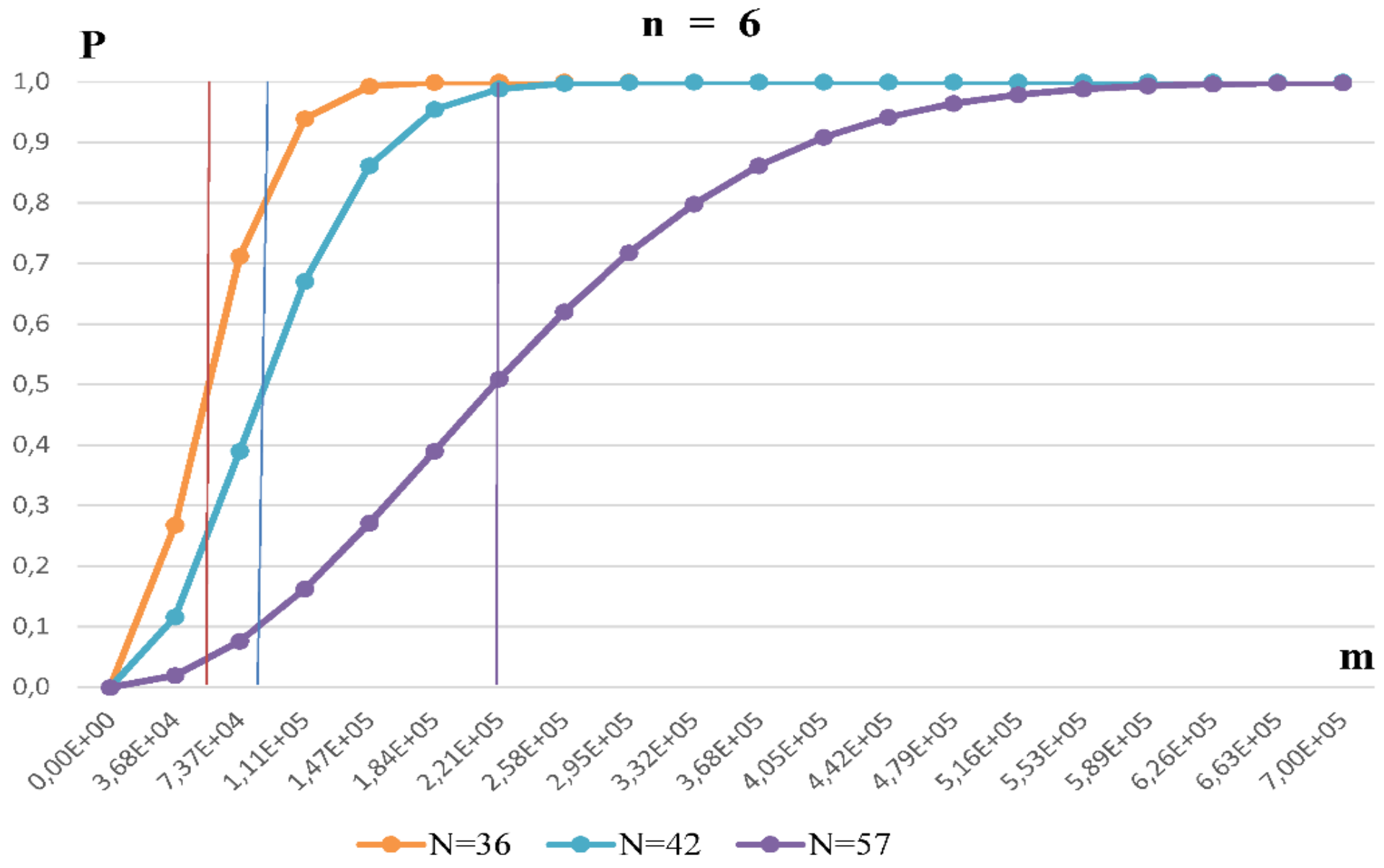
длина пароля $n = 6, 7, 8$;

количество пользователей m – от 1 до $1{,}7 \cdot 10^7$.

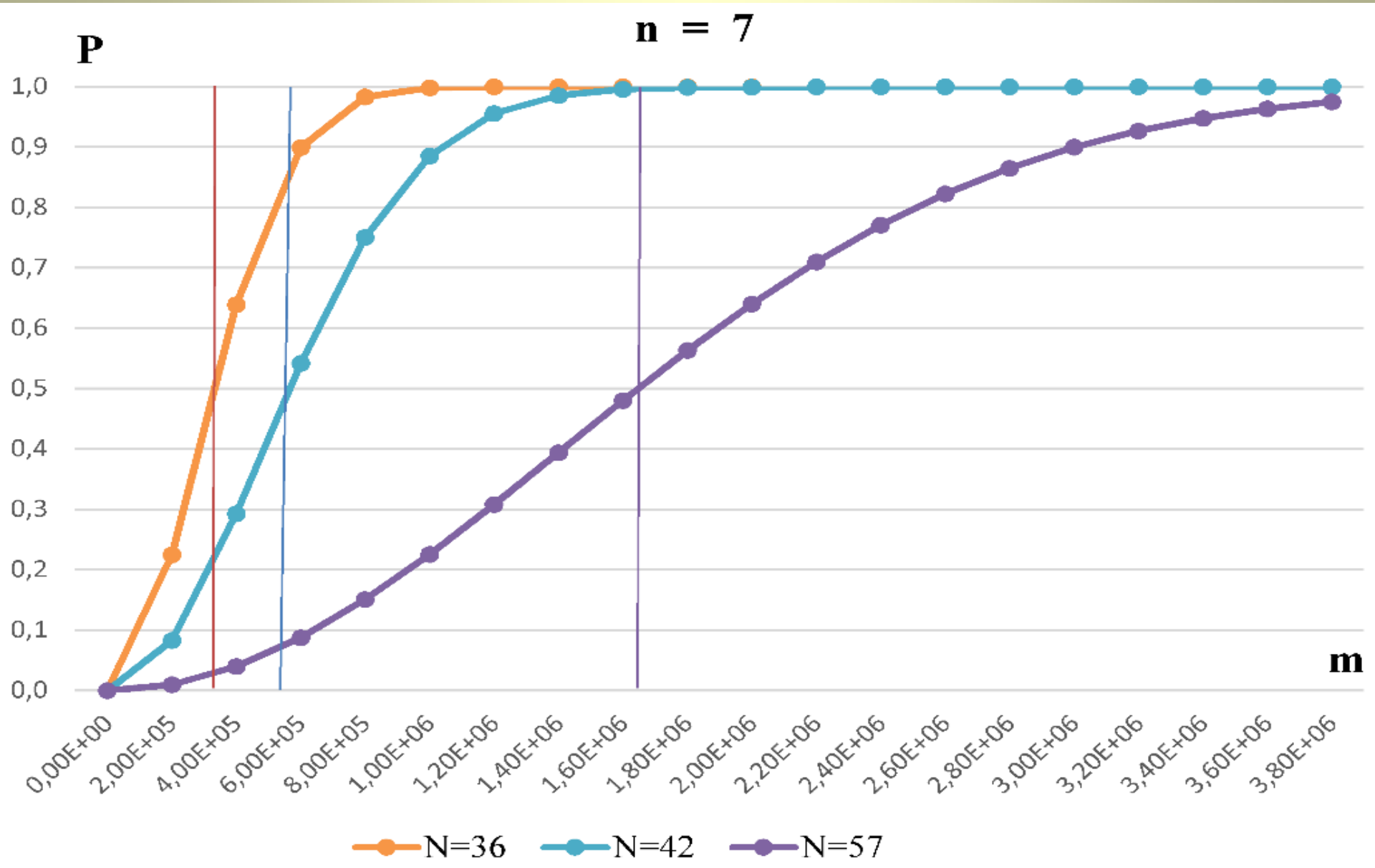
Для приближенного вычисления значения факториала $n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ и расчета полученной функции использовалась формула Стирлинга :

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

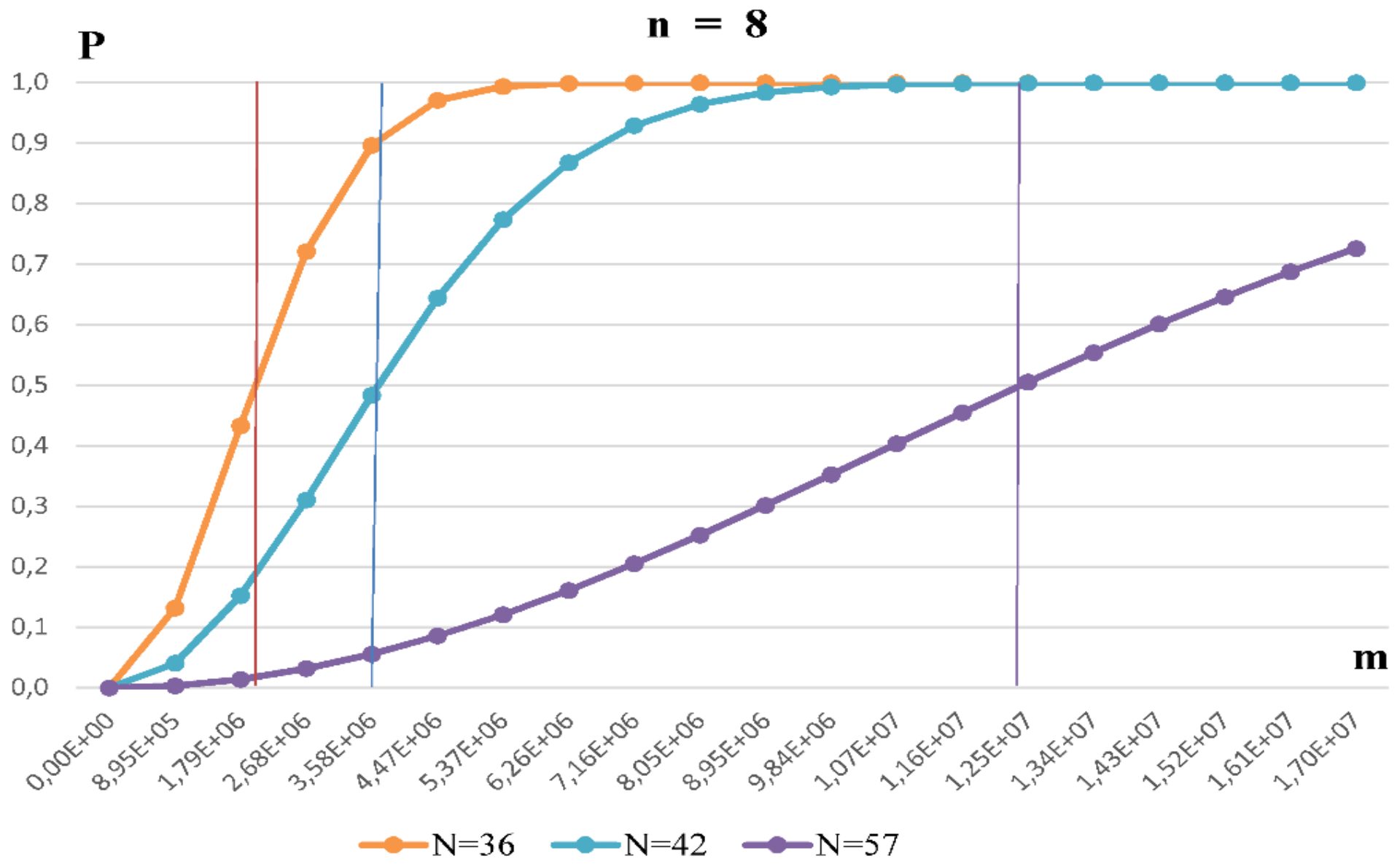
Стойкость механизмов аутентификации в инфокоммуникационных сетях



Стойкость механизмов аутентификации в инфокоммуникационных сетях



Стойкость механизмов аутентификации в инфокоммуникационных сетях



Стойкость механизмов аутентификации в инфокоммуникационных сетях

По отношению к атаке «день 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.

$$P(m) < 0,5. \quad (4)$$

С другой стороны, парольная система аутентификации считается не стойкой, если величина вероятности совпадения двух назначаемых в ней паролей

$$P(m) \geq 0,5.$$

Данные о количестве пользователей, соответствующих принятому критерию, на рис. 1–3. отмечены вертикальными линиями и приведены в табл. 1. Для указанных параметров системы с числом пользователей, расположенных слева от прямых, являются не стойкими.

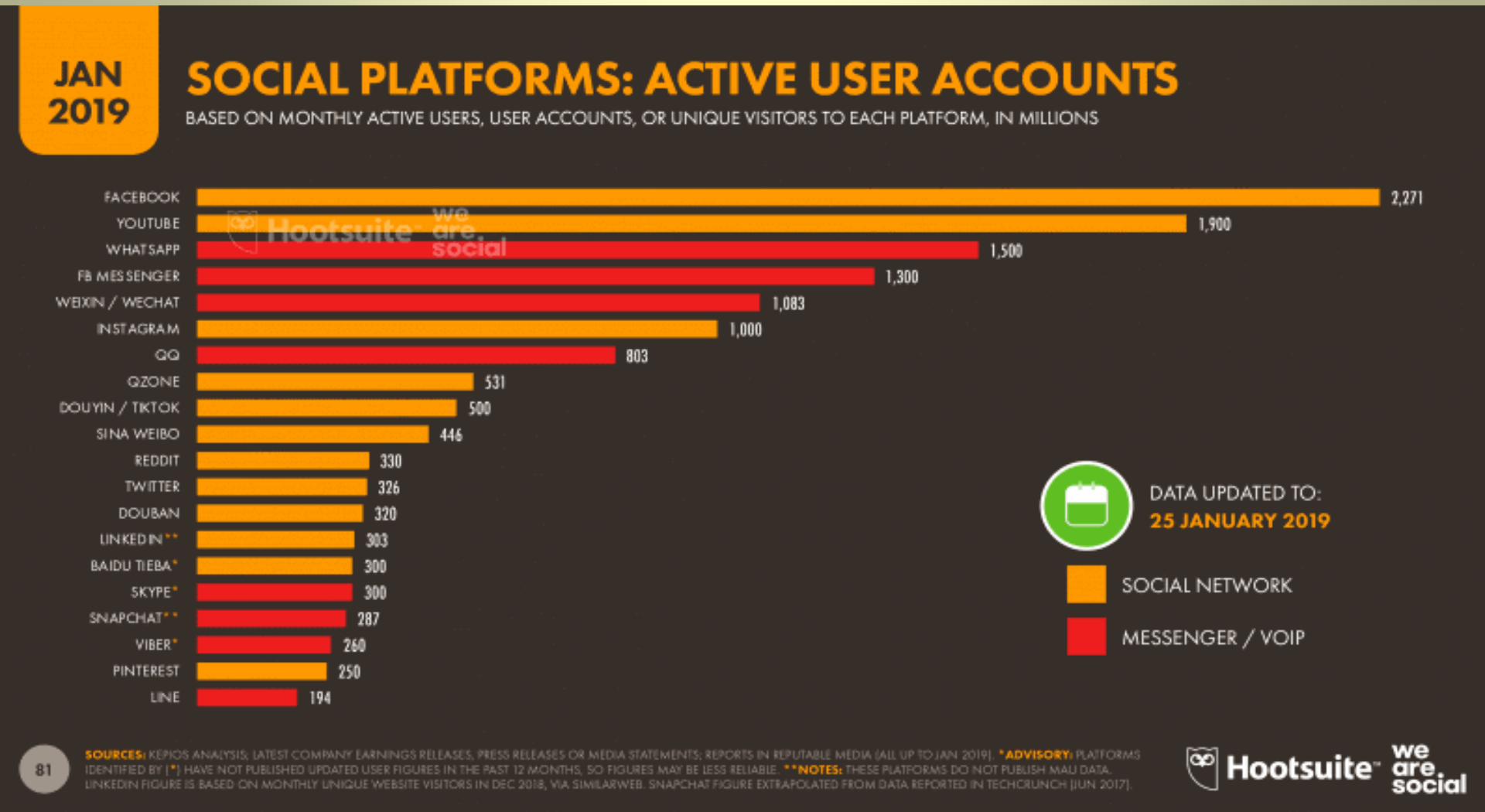
Стойкость механизмов аутентификации в инфокоммуникационных сетях

Таблица 1

№ п/п	Размер алфавита		$P(m) = 0{,}5$			$P(m) = 0{,}9$	
			n			n	
		6	7	8	6	7	8
1	36	$3{,}7.10^4$	$4{,}0.10^5$	$1{,}8.10^6$	$1{,}1.10^5$	$6{,}0.10^5$	$3{,}5.10^6$
2	42	$9{,}5.10^4$	$6{,}0.10^5$	$3{,}5.10^6$	$1{,}8.10^5$	$1{,}2.10^6$	$7{,}2.10^6$
3	57	$2{,}2.10^5$	$1{,}6.10^6$	$1{,}3.10^7$	$4{,}0.10^5$	$3{,}0.10^6$	$\sim 10^9$

Стойкость механизмов аутентификации в инфокоммуникационных сетях

Оценим стойкость наиболее распространённых социальных сетей, данные по которым приводятся в исследовании компании «WebCanape» от января 2019 года.



Стойкость механизмов аутентификации в инфокоммуникационных сетях

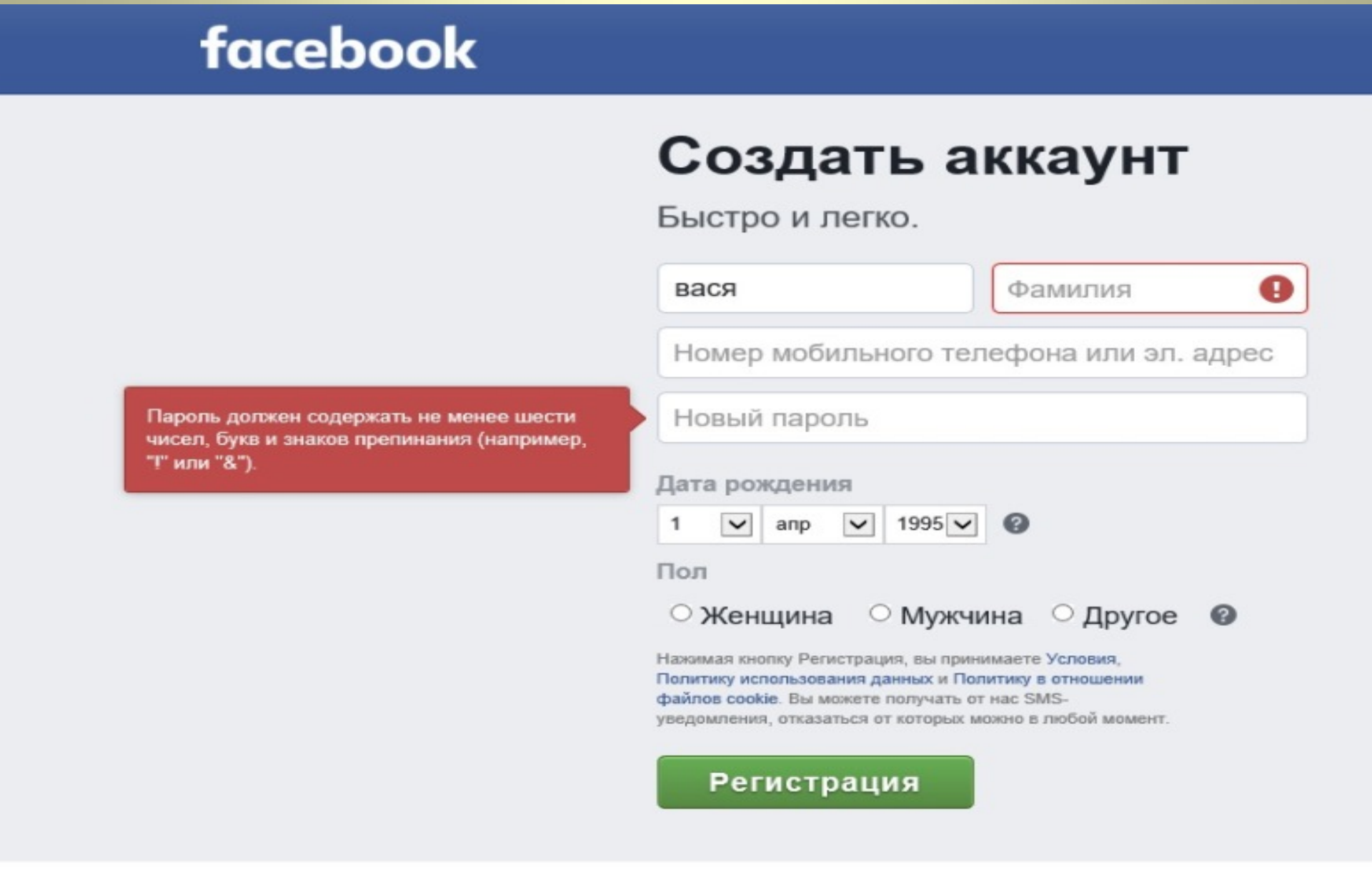
Количество учётных записей пользователей наиболее распространённых социальных сетей представлено в табл. 2:

Таблица 2

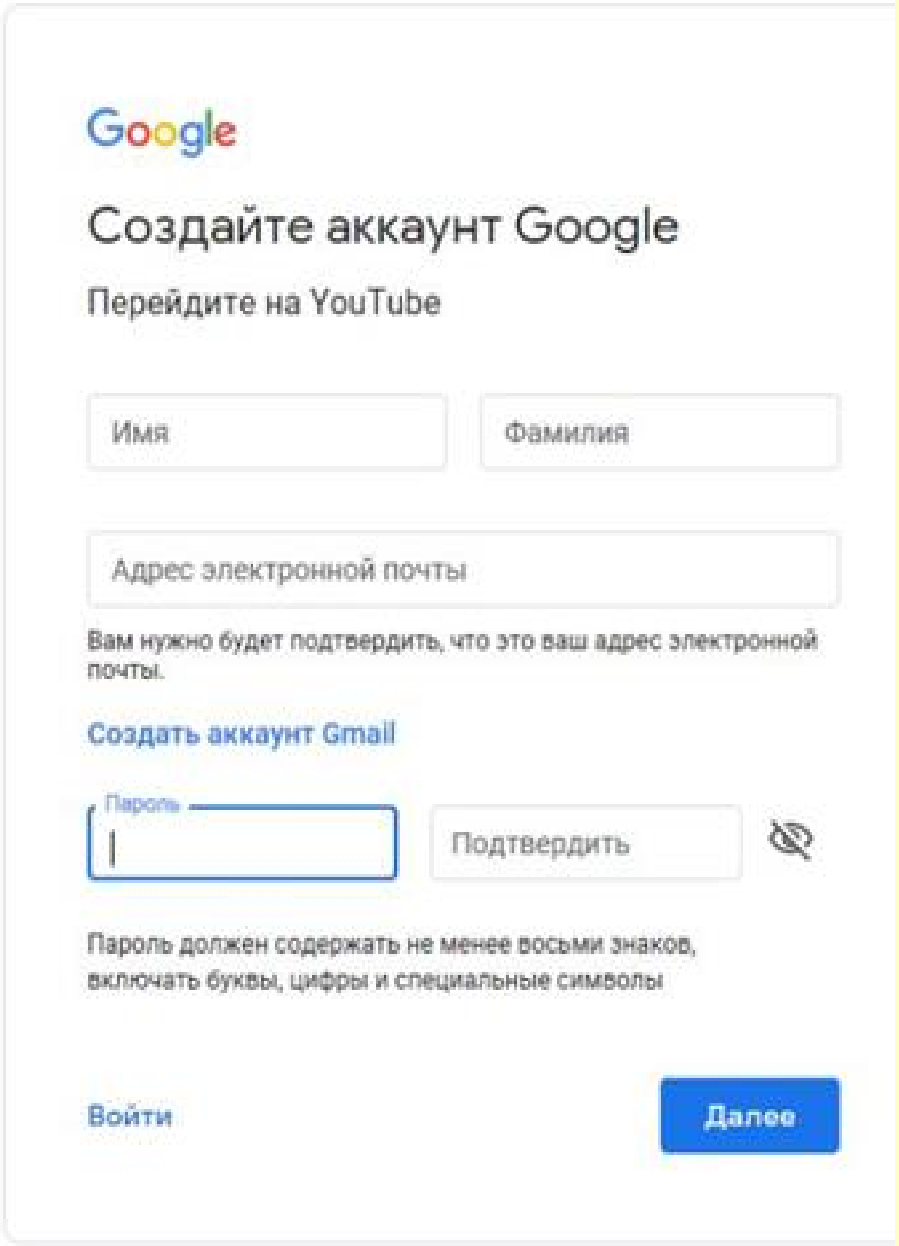
№ п/п	Наименование сети	Количество пользователей
1	Facebook	2,27млрд. = $2{,}27 \cdot 10^9$
2	YouTube	1,9 млрд. = $1{,}9 \cdot 10^9$
3	Instagram	1,0 млрд. = $1{,}0 \cdot 10^9$
4	Ozone	536 млн. = $5{,}31 \cdot 10^8$
5	Twitter	326 млн. = $3{,}26 \cdot 10^8$
6	LinkedIn	303 млн. = $3{,}03 \cdot 10^8$

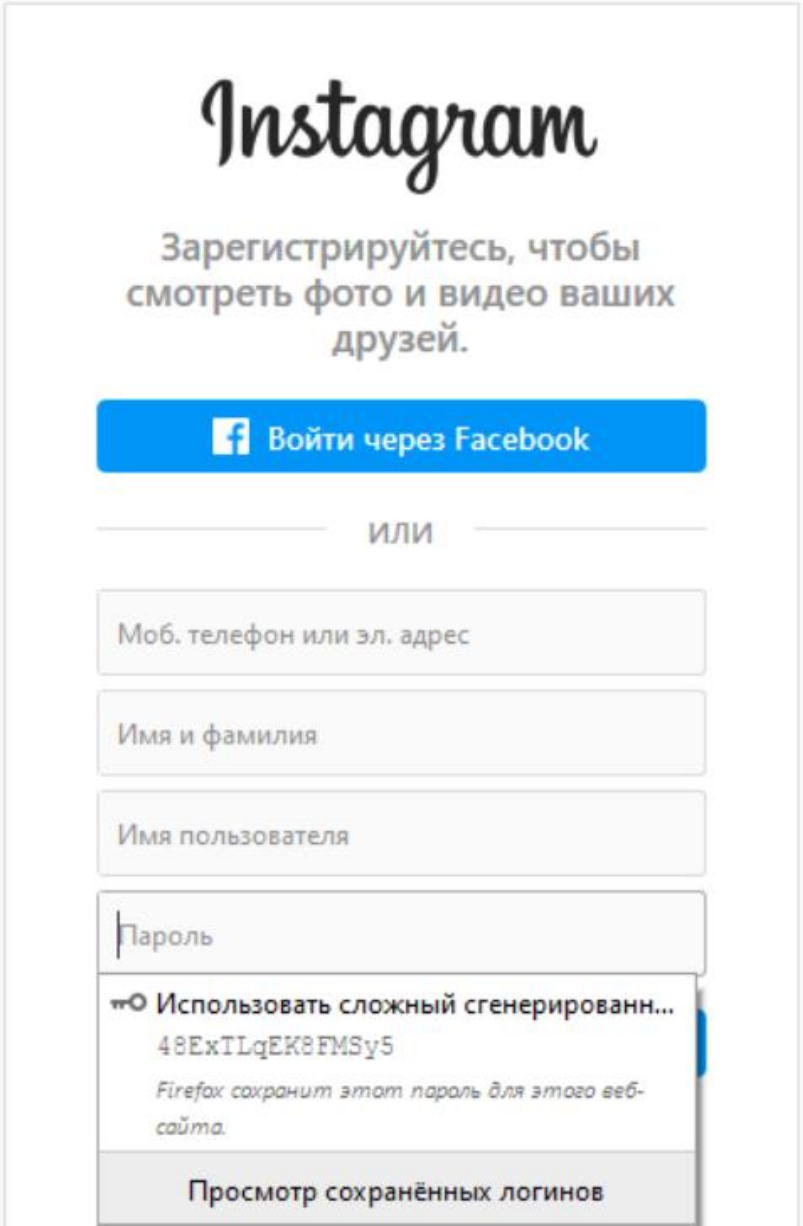
При регистрации указанные сети предъявляют различные требования к паролям, как, например, приведенные на рисунках ниже.

Стойкость механизмов аутентификации в инфокоммуникационных сетях



Стойкость механизмов аутентификации в инфокоммуникационных сетях





Стойкость механизмов аутентификации в инфокоммуникационных сетях

Минимально необходимые параметры парольных систем аутентификации, используемые в распространённых социальных сетях приведены в табл. 3.

Таблица 3

№ п/п	Наименование сети	Количество пользователей	Алфавит A	Длина пароля n	$P_{П1}$
1	Facebook	$2{,}27.10^9$	42	6	$5{,}5.10^9$
2	YouTube	$1{,}9.10^9$	42	8	$9{,}6.10^{12}$
3	Instagram	$1{,}0.10^9$	62	15	$4{,}8.10^{28}$
4	Ozone	$5{,}31.10^8$	36	6	$2{,}1.10^9$
5	Twitter	$3{,}26.10^8$	36	6	$2{,}1.10^9$
6	LinkedIn	$3{,}03.10^8$	36	6	$2{,}1.10^9$

Стойкость механизмов аутентификации в инфокоммуникационных сетях

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 «день рождения» приведены в табл. 4.

Таблица 4

№ п/п	Наименование сети	Количество пользователей	Количество пользователей по критерию $P(m) = 0{,}5$	$P_{П1}$	
1	Facebook	$2{,}27.10^9$	$9{,}5.10^4$	$5{,}5.10^9$	-
2	YouTube	$1{,}9.10^9$	$3{,}6.10^6$	$9{,}6.10^{12}$	-
3	Instagram	$1{,}0.10^9$	$\sim 10^{12}$	$4{,}8.10^{28}$	Соотв.
4	Ozone	$5{,}31.10^8$	$3{,}7.10^4$	$2{,}1.10^9$	-
5	Twitter	$3{,}26.10^8$	$3{,}7.10^4$	$2{,}1.10^9$	-
6	LinkedIn	$3{,}03.10^8$	$3{,}7.10^4$	$2{,}1.10^9$	-

Стойкость механизмов аутентификации в инфокоммуникационных сетях

Для практического расчёта стойкости сети к атаке «день рождения» используется следующее упрощённое аналитическое выражение

$$m = A^{\frac{n}{2}}.$$

Таким образом, парольные системы аутентификации, используемые в больших распределённых сетях, в которых число пользователей m сравнимо или больше возможного количества выбираемых ими для доступа к услугам аутентификаторов N, должны оцениваться на стойкость к атаке «день рождения» в соответствии с критерием:

$$m = A^{\frac{n}{2}}.$$

СПАСИБО ЗА ВНИМАНИЕ !