

Контрольная работа.

1. Выбор варианта

Вариант выбирается из таблицы по сумме последних 3-х цифр зачетки.

Для исходного алфавита будем использовать только английский набор символов, тогда мощность исходного алфавита будет:

Исходный алфавит	Мощность алфавита
Цифры от 0 до 9	10
Цифры от 0 до 9 и спецсимволы	10
Маленькие буквы (англ.)	26
Большие буквы (англ.)	26
Цифры и маленькие буквы	36
Цифры, маленькие и большие буквы	62
Цифры, маленькие и большие буквы и спецсимволы	72

№ варианта	A – мощность алфавита	L – длина пароля	V – скорость перебора паролей злоумышленником	T – срок действия паролей, в сутках
1	10	6	10^7	30
2	26	10	10^7	10
3	36	14	10^9	15
4	62	10	10^5	20
5	72	5	10^6	90
6	10	8	10^{20}	60
7	26	9	10^{16}	30
8	36	13	10^{10}	20
9	62	11	10^{14}	15
10	72	15	10^{25}	10
11	10	20	10^7	7
12	26	8	10^7	9
13	36	9	10^9	20
14	62	6	10^5	30
15	72	4	10^6	60
16	10	12	10^{20}	25
17	26	13	10^{16}	50
18	36	14	10^{10}	40
19	62	7	10^{14}	70
20	72	10	10^{25}	35
21	10	9	10^6	28
22	26	13	10^{10}	30
23	36	14	10^{14}	20
24	62	12	10^{25}	40
25	72	13	10^{16}	30
26	10	16	10^{16}	50
27	62	9	10^{14}	20

Вероятность подбора паролей злоумышленником, можно привести в следующем виде:

$$P(t < T) = \begin{cases} \frac{V \cdot T}{A^L}, & V \cdot T < A^L; \\ 1, & V \cdot T \geq A^L. \end{cases}$$

A – мощность алфавита символов, из которых состоит пароль;

L – длина пароля, символов;

V – скорость перебора паролей злоумышленником, паролей/секунду;

T – срок действия паролей, в секундах. Обычно задается в сутках, поэтому нужно умножить на количество секунд в сутках – 86400 с.;

P – вероятность подбора паролей злоумышленником за время t, меньшее срока действия паролей.