МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт информационных технологий (ИИТ)
Кафедра информационных технологий в атомной энергетике (ИТАЭ)

ОТЧЕТ ПО ВЫПОЛНЕНИЮ КОМПЛЕКСНОЙ ЗАДАЧИ

по дисциплине «Моделирование безопасности компьютерных систем»

Вариант: 6

Студент группы *ИКБО-50-23 Павлов Н.С.* _____ (подпись)

Доцент *Баричев С.Г.* _____ (подпись)

Москва 2025 г.

СОДЕРЖАНИЕ

1. ПОСТАНОВКА ЗАДАЧИ

Автоматизированная система управления объекта ядерной энергетики включает трехуровневую подсистему защиты с тремя звеньями на каждом уровне.

У1. Защита от воздействия ошибочных команд управления.

Угроза: ошибочно сформированная команда, не обнаруживаемая декодером.

Средство защиты: подсистема обнаружения ошибок

Последствие: возможность манипуляции с системой защиты

Показатель защищенности: Вероятность обнаружения ошибки – $P_{У1}$

У2. Модуль аутентификации пользователя по паролю

Угроза: подбор пароля (автоматизированный подбор пароля)

Средство защиты: подсистема аутентификации

Последствие: возможность запуска компьютерного вируса

Показатель защищенности: Вероятность НЕподбора пароля – $P_{У2}$

У3. Воздействие компьютерной эпидемии (сценарий пандемии без карантина)

Угроза: заражение и выход из строя компьютеров

Средство защиты: антивирусная подсистема

Последствие: дезорганизация системы управления объектом ядерной энергетики

Показатель защищенности: Доля незараженных компьютеров – $P_{У3}$

Задание:

1. Рассчитать вероятность нарушения системы защиты при одиночном и групповом воздействии
2. Исследовать зависимость эффективности системы защиты против одиночного и группового воздействия при изменении одного из параметров элемента защиты (у каждого варианта – свой параметр и свой диапазон для исследований)

2 ВЫПОЛНЕНИЕ РАБОТЫ

Для расчета защищенности системы и последующего исследования ее зависимости от параметров системы исследуем эффективность защиты каждого из трех уровней: $P_{У1}$, $P_{У2}$, $P_{У3}$

2.1 Расчет эффективности подсистемы обнаружения ошибок $P_{У1}$

Для защиты АСУ от ошибок в подсистеме защиты предусмотрены декодеры ошибок на каждом из трех входящих каналов управления на основе линейных помехоустойчивых кодов.

Каждый из них задается своей порождающей матрицей, которая и определяет эффективность конкретного звена $P_{У1}^{i}$, которая рассчитывается как вероятность обнаружения ошибки данным декодером (их три).

Вероятность обнаружения ошибки определяется формулой

$$P_{обн} = 1 - (A_1 p q^{n-1} + A_2 p_2 q^{n-2} + A_3 p^3 q^{n-3} + \ldots + A_n p^n)$$

где

- p – вероятность одиночной ошибки,
- $q = 1 - p$
- n – длина кодового вектора
- A_i – спектральный коэффициент

Исходные данные:

Декодер канала-1:

(9,4)-код с порождающей матрицей:

G	1	0	0	0	0	0	1	1	0
	0	1	0	0	1	1	0	0	1
	0	0	1	0	1	0	1	1	0
	0	0	0	1	1	1	0	1	1

Рисунок 1 – Порождающая матрица

$p = 0{,}0106$

Декодер канала-2:

(9,5)-код с порождающей матрицей

G	1	0	0	0	0	0	1	1	0
	0	1	0	0	1	1	0	0	1
	0	0	1	0	1	0	1	1	0
	0	0	0	1	1	1	0	1	1
	0	0	0	0	1	1	1	0	1

Рисунок 2 – Порождающая матрица

$p = 0{,}0206$

Декодер канала-3:

(9,3)-код с порождающей матрицей

G	1	0	0	0	0	0	1	1	0
	0	1	0	0	1	1	0	0	1
	0	0	1	0	1	0	1	1	0

Рисунок 3 – Порождающая матрица

$p = 0{,}106$

Результаты расчета:

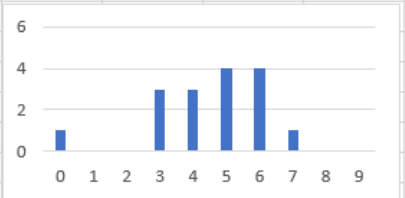
- $P_{УI}{}^{1} = 0{,}999997$
- $P_{УI}{}^{2} = 0{,}999219$
- $P_{УI}{}^{3} = 0{,}999998$

G	1	0	0	0	0	0	1	1	0
	0	1	0	0	1	1	0	0	1
	0	0	1	0	1	0	1	1	0
	0	0	0	1	1	1	0	1	1

Кодовые векторы														Вес
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1	1	1	0	1	1		5
0	0	1	0	0	0	1	0	1	0	1	1	0		4
0	0	1	1	0	0	1	1	0	1	1	0	1		5
0	1	0	0	0	1	0	0	1	1	0	0	1		4
0	1	0	1	0	1	0	1	0	0	0	1	0		3
0	1	1	0	0	1	1	0	0	1	1	1	1		6
0	1	1	1	0	1	1	1	1	0	1	0	0		5
1	0	0	0	1	0	0	0	0	0	1	1	0		3
1	0	0	1	1	0	0	1	1	1	1	0	1		6
1	0	1	0	1	0	1	0	1	0	0	0	0		3
1	0	1	1	1	0	1	1	0	1	0	1	1		6
1	1	0	0	1	1	0	0	1	1	1	1	1		7
1	1	0	1	1	1	0	1	0	0	1	0	0		4
1	1	1	0	1	1	1	0	0	1	0	0	1		5
1	1	1	1	1	1	1	1	1	0	0	1	0		6

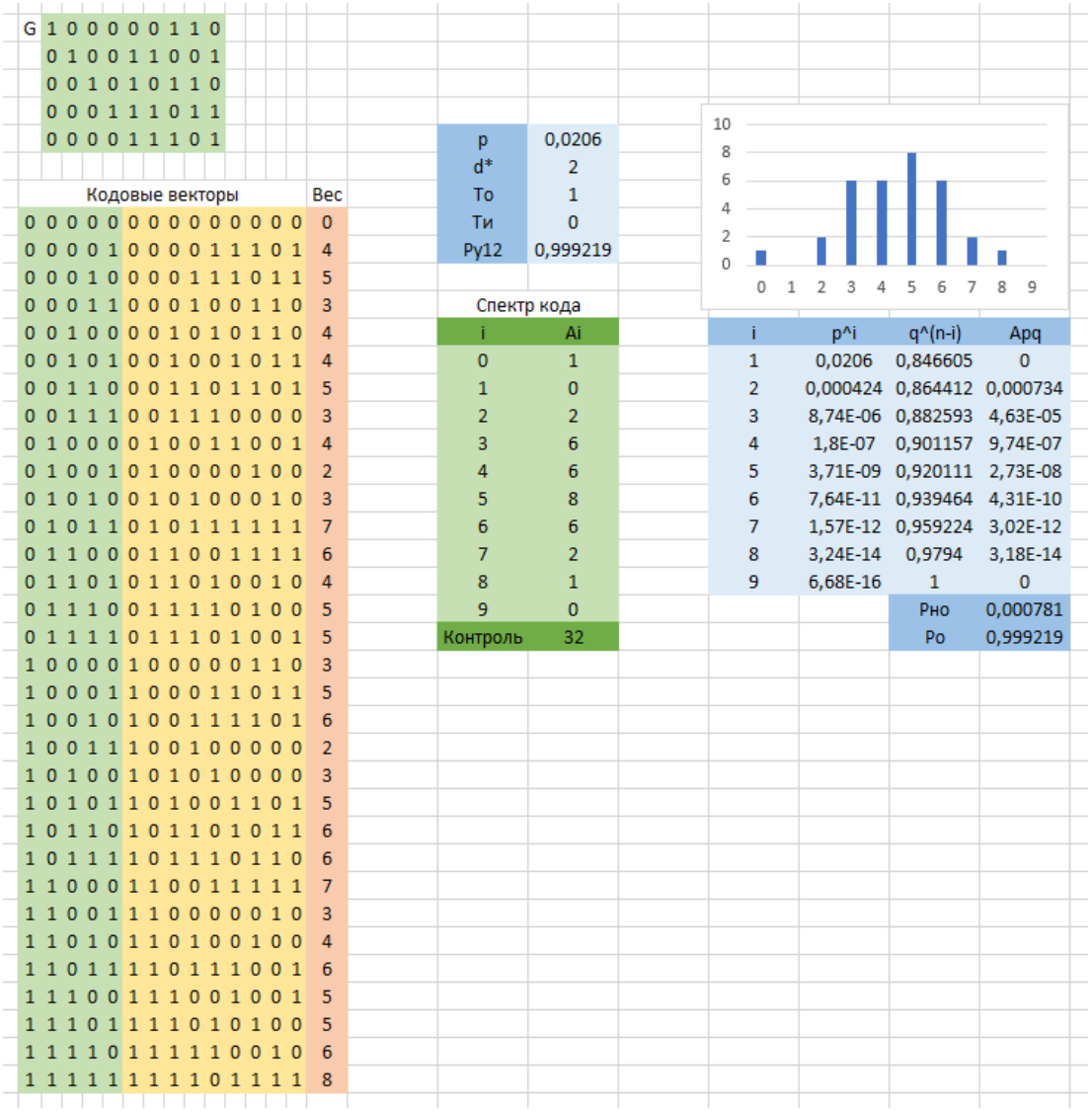
p	0,0106
d*	3
To	2
Ти	1
Ру11	0,999997

Спектр кода	
i	Ai
0	1
1	0
2	0
3	3
4	3
5	4
6	4
7	1
8	0
9	0
Контроль	16



i	p^i	q^(n-i)	Apq
1	0,0106	0,91828	0
2	0,000112	0,928118	0
3	1,19E-06	0,938062	3,35E-06
4	1,26E-08	0,948112	3,59E-08
5	1,34E-10	0,958269	5,13E-10
6	1,42E-12	0,968536	5,5E-12
7	1,5E-14	0,978912	1,47E-14
8	1,59E-16	0,9894	0
9	1,69E-18	1	0
		Рно	3,39E-06
		Ро	0,999997

Рисунок 4 – Расчет эффективности декодера канала-1



G								
1	0	0	0	0	0	1	1	0
0	1	0	0	1	1	0	0	1
0	0	1	0	1	0	1	1	0
0	0	0	1	1	1	0	1	1
0	0	0	0	1	1	1	0	1

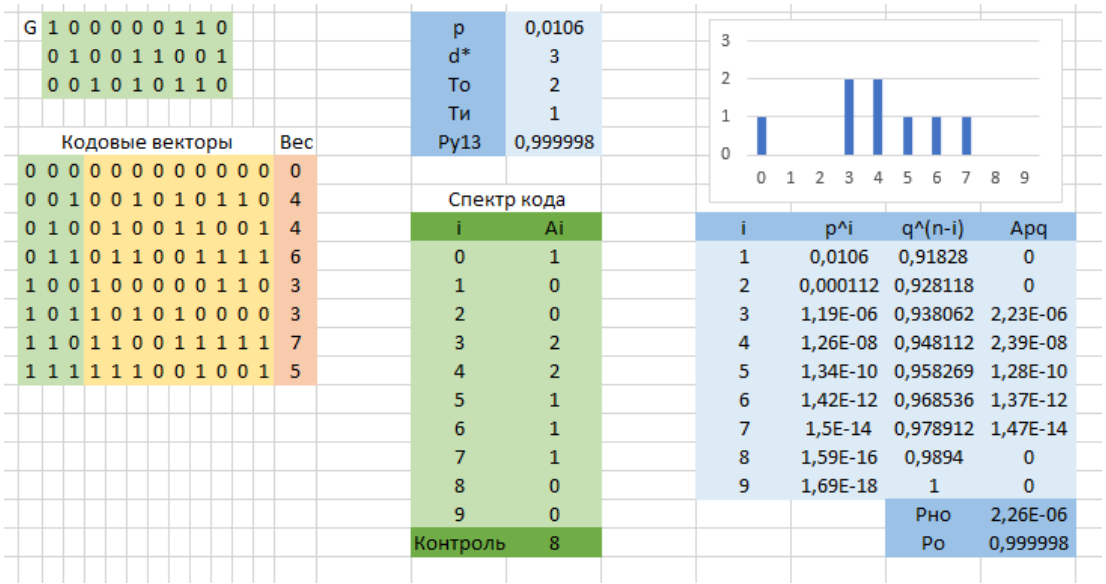
Кодовые векторы														Вес
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	1	1	1	0	1	4
0	0	0	1	0	0	0	0	1	1	1	0	1	1	5
0	0	0	1	1	0	0	0	1	0	0	1	1	0	3
0	0	1	0	0	0	0	1	0	1	0	1	1	0	4
0	0	1	0	1	0	0	1	0	0	1	0	1	1	4
0	0	1	1	0	0	0	1	1	0	1	1	0	1	5
0	0	1	1	1	0	0	1	1	1	0	0	0	0	3
0	1	0	0	0	0	1	0	0	1	1	0	0	1	4
0	1	0	0	1	0	1	0	0	0	0	1	0	0	2
0	1	0	1	0	0	1	0	1	0	0	0	1	0	3
0	1	0	1	1	0	1	0	1	1	1	1	1	1	7
0	1	1	0	0	0	1	1	0	0	1	1	1	1	6
0	1	1	0	1	0	1	1	0	1	0	0	1	0	4
0	1	1	1	0	0	1	1	1	1	0	1	0	0	5
0	1	1	1	1	0	1	1	1	0	1	0	0	1	5
1	0	0	0	0	1	0	0	0	0	0	1	1	0	3
1	0	0	0	1	1	0	0	0	1	1	0	1	1	5
1	0	0	1	0	1	0	0	1	1	1	1	0	1	6
1	0	0	1	1	1	0	0	1	0	0	0	0	0	2
1	0	1	0	0	1	0	1	0	1	0	0	0	0	3
1	0	1	0	1	1	0	1	0	0	1	1	0	1	5
1	0	1	1	0	1	0	1	1	0	1	0	1	1	6
1	0	1	1	1	1	0	1	1	1	0	1	1	0	6
1	1	0	0	0	1	1	0	0	1	1	1	1	1	7
1	1	0	0	1	1	1	0	0	0	0	0	1	0	3
1	1	0	1	0	1	1	0	1	0	0	1	0	0	4
1	1	0	1	1	1	1	0	1	1	1	0	0	1	6
1	1	1	0	0	1	1	1	0	0	1	0	0	1	5
1	1	1	0	1	1	1	1	0	1	0	1	0	0	5
1	1	1	1	0	1	1	1	1	1	0	0	1	0	6
1	1	1	1	1	1	1	1	1	0	1	1	1	1	8

p	0,0206
d*	2
To	1
Ти	0
Ру12	0,999219

Спектр кода	
i	Ai
0	1
1	0
2	2
3	6
4	6
5	8
6	6
7	2
8	1
9	0
Контроль	32

i	p^i	q^(n-i)	Apq
1	0,0206	0,846605	0
2	0,000424	0,864412	0,000734
3	8,74E-06	0,882593	4,63E-05
4	1,8E-07	0,901157	9,74E-07
5	3,71E-09	0,920111	2,73E-08
6	7,64E-11	0,939464	4,31E-10
7	1,57E-12	0,959224	3,02E-12
8	3,24E-14	0,9794	3,18E-14
9	6,68E-16	1	0
		Рно	0,000781
		Ро	0,999219

Рисунок 5 – Расчет эффективности декодера канала-2



G								
1	0	0	0	0	0	1	1	0
0	1	0	0	1	1	0	0	1
0	0	1	0	1	0	1	1	0

Кодовые векторы												Вес
0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	1	0	1	0	1	1	0	4
0	1	0	0	1	1	0	0	1	1	0	0	4
0	1	1	0	1	1	0	0	1	1	1	1	6
1	0	0	1	0	0	0	0	0	1	1	0	3
1	0	1	1	0	1	0	1	0	0	0	0	3
1	1	0	1	1	0	0	1	1	1	1	1	7
1	1	1	1	1	1	0	0	1	0	0	1	5

p	0,0106
d*	3
To	2
Ти	1
Ру13	0,999998

Спектр кода	
i	Ai
0	1
1	0
2	0
3	2
4	2
5	1
6	1
7	1
8	0
9	0
Контроль	8

i	p^i	q^(n-i)	Apq
1	0,0106	0,91828	0
2	0,000112	0,928118	0
3	1,19E-06	0,938062	2,23E-06
4	1,26E-08	0,948112	2,39E-08
5	1,34E-10	0,958269	1,28E-10
6	1,42E-12	0,968536	1,37E-12
7	1,5E-14	0,978912	1,47E-14
8	1,59E-16	0,9894	0
9	1,69E-18	1	0
		Рно	2,26E-06
		Ро	0,999998

Рисунок 6 – Расчет эффективности декодера канала-3

2.2 Расчет эффективности подсистемы аутентификации

Эффективность подсистемы аутентификации определяется вероятностью неподбора пароля, необходимого для преодоления этого уровня защиты. В заданной системе действуют три средства аутентификации, преодоление путем побора пароля любого из них означает преодоление всего уровня.

Вероятность p подбора ключа длиной L из алфавита объемом M с n попыток определяется по формуле:

$$p = n / M^L$$

У злоумышленника есть возможность перебирать пароли автоматизированным образом в течение времени t (с) со скоростью v (паролей/с). Тогда

$$p = vt / M^L$$

Если p, вычисленный согласно этой формуле, равен числу больше единицы, то принимается $p = 1$ (гарантированный подбор)

Тогда эффективность каждого i-го средства аутентификации определяется как:

$$P_{y2}{}^i = 1 - v_i t / M_i^{Li}$$

Параметры Mi, Li, vi, t для трех средств аутентификации заданы (в таблице на рис.7). Результаты расчета эффективности средств аутентификации представлены на рис.7:

№ средства аутентификации	Mi	Li	vi	t	Py2i
1	128	9	1548	19144	1
2	64	7	2950	19144	0,999987
3	68	11	1575	19144	1

Рисунок 7 – Результаты расчета $P_{y2}{}^i$

2.3 Расчет эффективности антивирусной защиты

Третий уровень защиты образуют средства антивирусной защиты. Показателем эффективности антивирусной защиты является доля незараженных компьютеров (в интервале от 0 до 1) через время T после начала заражения, которое становится возможным с преодолением уровня аутентификации.

В нашем случае используется модель пандемии без карантина и иммунизации. Вероятность заражения компьютера в следующий момент модельного времени зависит от числа уже зараженных компьютеров, вероятности заражения при контакте, а также связности сети.

Предполагается, что противник запускает три разных компьютерных вирусов, от которых система защиты имеет разную эффективность.

Для каждого из вирусов расчет эффективности делается исходя из следующей модели.

Пусть имеются исходные данные:

- N_0 – начальное количество зараженных узлов (20, 2, 10)
- K_c – коэффициент связности сети (4, 7, 5)
- $P_з$ – вероятность заражения при контакте узлов на одном шаге (0.2, 0.17, 0.28)
- N – общее число узлов сети (900, 680, 460)
- T – время действия эпидемии (4)

Обозначим:

- $N_i^Б$ – число зараженных узлов на i-м шаге
- $N_i^З$ – число «здоровых» узлов на i-м шаге

Очевидно, что

$$N_i^Б + N_i^З = N$$

Тогда динамика эпидемии будет определяться следующей моделью:

$$N_i^Б = N_{i-1}^Б + N_{i-1}^Б * K_c * P_з * (N_{i-1}^З / N)$$

Используя эту модель проведем исследование динамики эпидемии каждого из трех вирусов.

Важно:

1) сумма второго и третьего столбца должна быть всегда равна N
2) количество больных и зараженных компьютеров округляются до целого
3) если количество здоровых компьютеров становится отрицательным, то с этого момента времени оно принимается за ноль (полное заражение сети).

По результатам исследования рассчитывается эффективность защиты против каждого из вирусов:

$$P_{y3} = (N_{10}^{3} / N)$$

Результаты расчета:

- $P_{y3}^{1} = 0{,}79209$
- $P_{y3}^{2} = 0{,}93431$
- $P_{y3}^{3} = 0{,}45791$

			i	Niб	Niз
Общее количество	900		0	20	880
Начальное заражение	20		1	36	864
Связность	4		2	63	837
Вер-ть заражени	0,2		3	110	790
Ру31	0,79209		4	187	713

			i	Niб	Niз
Общее количество	680		0	2	678
Начальное заражение	2		1	4	676
Связность	7		2	10	670
Вер-ть заражени	0,17		3	21	659
Ру32	0,93431		4	45	635

			i	Niб	Niз
Общее количество	460		0	10	450
Начальное заражение	10		1	24	436
Связность	5		2	55	405
Вер-ть заражени	0,28		3	123	337
Ру33	0,45791		4	249	211

Рисунок 8 – Результаты расчета P_{y3}^{i}

2.4 Расчет эффективности всей подсистемы защиты против одиночного и группового воздействия

Групповой нарушитель (воздействие) – нарушитель, имеющий возможность атаковать все звенья одного уровня одновременно.

Защищенность многоуровневой системы (вероятность непреодоления нарушителем/угрозой всех уровней защиты) определяется формулой:

$$P_C = 1 – (1 – P_{У1}) (1 – P_{У2})(1 – P_{У3}),$$

где $P_{Уi}$ – защищенность i-го многозвенного уровня.

Защищенность многозвенного уровня определяется формулами:

а) для одиночного нарушителя:

$$P_o = min (P_{Уi}^1 , P_{Уi}^2, P_{Уi}^3),$$

где $P_{Уi}^j$ – защищенность j-го звена i-го уровня, рассчитанная выше.

б) для группового нарушителя:

$$P_г = P_{Уi}^1 * P_{Уi}^2 * P_{Уi}^3.$$

Для всей системы проверкой служит факт того, что защищенность системы от группового нарушителя должна быть меньше защищенности системы от одиночного нарушителя.

Результаты расчета эффективности всей системы против одиночного и группового воздействия приведены в таблице:

	Звено 1	Звено 2	Звено 3	Po	Pг
Уровень 1	0,999997	0,999219	0,999998	0,999219062	0,99921342
Уровень 2	1	0,999987	1	0,999987159	0,999987159
Уровень 3	0,792087	0,93431	0,457909	0,457908589	0,338877246
Эффективность общая				0,999999995	0,999999993

Рисунок 9 – Таблица итоговых расчетов

2.5 Исследование зависимости эффективности всей подсистемы защиты против одиночного и группового воздействия при изменении параметра(v_2)

На основе созданных выше моделей можно провести исследование зависимости показателей *Po Pг*, подставляя в модель разные исходные данные. Результаты исследования приведены в таблице:

Исследуемый параметр v2	Po	Pr
2950	0,999999994563945	0,999999993322405
3000	0,999999994471808	0,999999993209225
3050	0,999999994379671	0,999999993096046
3100	0,999999994287535	0,999999992982866
3150	0,999999994195398	0,999999992869687

Рисунок 10 – Таблица исследования параметра v_2

На основе полученных данных можно построить график:

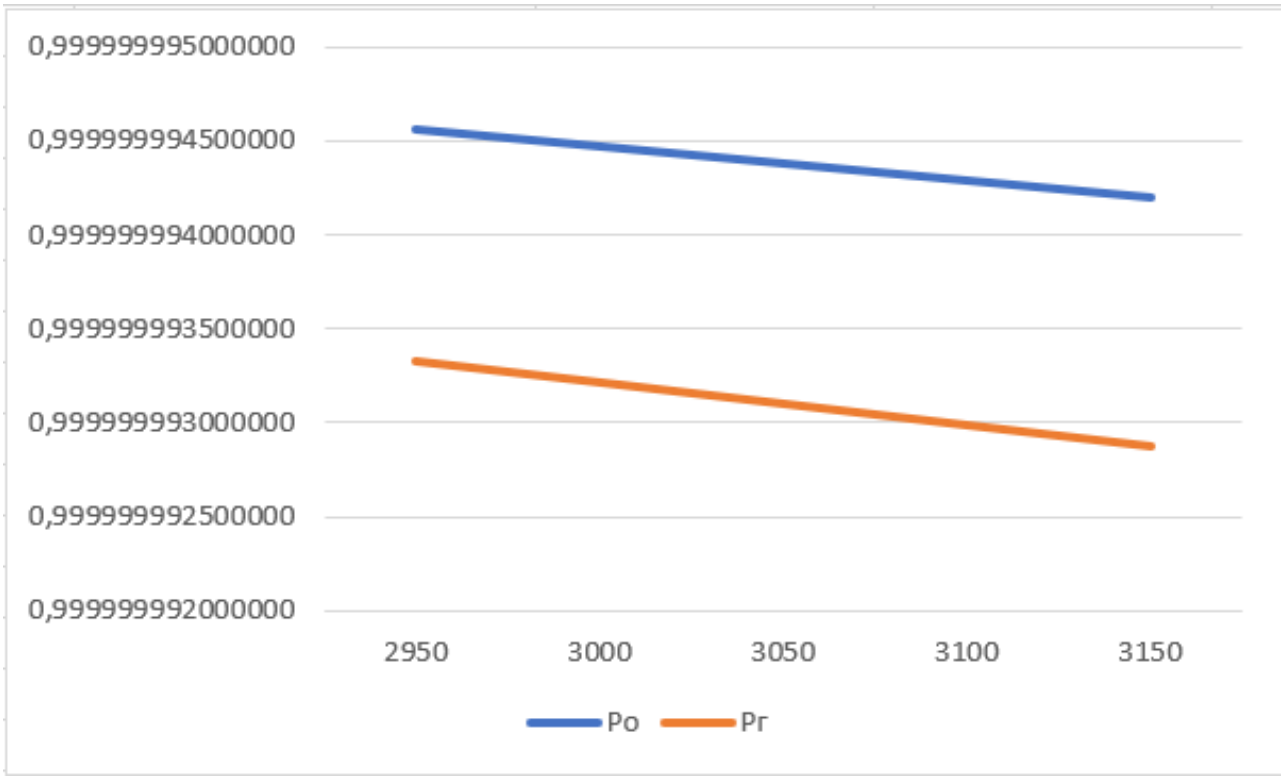


Рисунок 11 – График изменения значений

Вывод:

Изменение параметра защиты (v_2) уменьшает незначительно эффективность защиты.