МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Пояснительная записка к комплексной работе

Дисциплина: «Моделирование безопасности компьютерных систем»

Выполнил студент: Враженко Д.О.
Группа: ИКБО-50-23
Вариант: 26

Москва – 2025

КОМПЛЕКСНАЯ ЗАДАЧА:

Тема: «Расчет и исследование защищенности автоматизированной системы управления объектом ядерной энергетики»

Цель: исследование зависимости защищенности многоуровневой и многозвенной системы защиты объекта ядерной энергетики от параметров конкретных элементов управления.

СОДЕРЖАНИЕ И СТРУКТУРА ПОЯСНИТЕЛЬНОЙ ЗАПИСКИ

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 – $P_{у3}$.

Даны параметры элементов защиты (у каждого варианта – свои).

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. РЕШЕНИЕ ЗАДАНИЙ

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

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

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

$$G = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{vmatrix}$$

$p = 0{,}0126$

Декодер канала-2:
(9,5)-код с порождающей матрицей

$$G = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{vmatrix}$$

$p = 0{,}0226$

Декодер канала-3:
(9,3)-код с порождающей матрицей

$$G = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{vmatrix}$$

$p = 0{,}126$

Результаты расчета:

Расчет эффективности декодера канала-1:

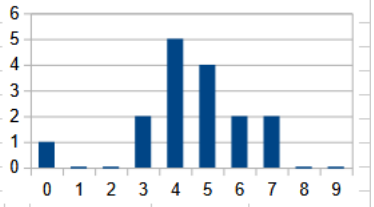
G=	1	0	0	0	1	1	0	1	0
	0	1	0	0	1	1	0	0	1
	0	0	1	0	1	0	1	1	0
	0	0	0	1	1	1	0	1	1

	Кодовые векторы									Вес
0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	1	1	0	1	1	5
2	0	0	1	0	1	0	1	1	0	4
3	0	0	1	1	0	1	1	0	1	5
4	0	1	0	0	1	1	0	0	1	4
5	0	1	0	1	0	0	0	1	0	3
6	0	1	1	0	0	1	1	1	1	6
7	0	1	1	1	1	0	1	0	0	5
8	1	0	0	0	1	1	0	1	0	4
9	1	0	0	1	0	0	0	0	1	3
10	1	0	1	0	0	1	1	0	0	4
11	1	0	1	1	1	0	1	1	1	7
12	1	1	0	0	0	0	0	1	1	4
13	1	1	0	1	1	1	0	0	0	5
14	1	1	1	0	1	0	1	0	1	6
15	1	1	1	1	0	1	1	1	0	7

p=	0,0126
d*=	3
To=	2
Ти=	1
Po=	0,999996173

СПЕКТР КОДА

i	*Ai*
0	1
1	0
2	0
3	2
4	5
5	4
6	2
7	2
8	0
9	0
контроль	16



i	*p^i*	*q^(n-i)*	*Apq*
1	0,0126	0,903535	0
2	0,00015876	0,9150648	0
3	2,000376E-06	0,9267418	3,707664E-06
4	2,520474E-08	0,9385677	1,182818E-07
5	3,175797E-10	0,9505446	1,207495E-09
6	4,001504E-12	0,9626743	7,70429E-12
7	5,041895E-14	0,9749588	9,83128E-14
8	6,352788E-16	0,9874	0
9	8,004513E-18	1	0
		Рно=	3,827161E-06
		Po=	0,999996173

$P_{У1}{}^{1} = P_O = 0{,}999996172838953$

Расчет эффективности декодера канала-2:

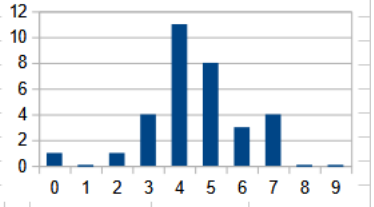
G=	1	0	0	0	1	1	0	1	0
	0	1	0	0	1	1	0	0	1
	0	0	1	0	1	0	1	1	0
	0	0	0	1	1	1	0	1	1
	0	0	0	0	1	1	1	0	1

	Кодовые векторы									Вес
0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	1	1	1	0	1	4
2	0	0	0	1	1	1	0	1	1	5
3	0	0	0	1	0	0	1	1	0	3
4	0	0	1	0	1	0	1	1	0	4
5	0	0	1	0	0	1	0	1	1	4
6	0	0	1	1	0	1	1	0	1	5
7	0	0	1	1	1	0	0	0	0	3
8	0	1	0	0	1	1	0	0	1	4
9	0	1	0	0	0	0	1	0	0	2
10	0	1	0	1	0	0	0	1	0	3
11	0	1	0	1	1	1	1	1	1	7
12	0	1	1	0	0	1	1	1	1	6
13	0	1	1	0	1	0	0	1	0	4
14	0	1	1	1	1	0	1	0	0	5
15	0	1	1	1	0	1	0	0	1	5
16	1	0	0	0	1	1	0	1	0	4
17	1	0	0	0	0	0	1	1	1	4
18	1	0	0	1	0	0	0	0	1	3
19	1	0	0	1	1	1	1	0	0	5
20	1	0	1	0	0	1	1	0	0	4
21	1	0	1	0	1	0	0	0	1	4
22	1	0	1	1	1	0	1	1	1	7
23	1	0	1	1	0	1	0	1	0	5
24	1	1	0	0	0	0	0	1	1	4
25	1	1	0	0	1	1	1	1	0	6
26	1	1	0	1	1	1	0	0	0	5
27	1	1	0	1	0	0	1	0	1	5
28	1	1	1	0	1	0	1	0	1	6
29	1	1	1	0	0	1	0	0	0	4
30	1	1	1	1	0	1	1	1	0	7
31	1	1	1	1	1	0	0	1	1	7

p=	0,0226
d*=	2
To=	1
Ти=	0
Po=	0,999521908

СПЕКТР КОДА

i	*Ai*
0	1
1	0
2	1
3	4
4	11
5	8
6	3
7	4
8	0
9	0
контроль	32



i	*p^i*	*q^(n-i)*	*Apq*
1	0,0226	0,8328728	0
2	0,00051076	0,852131	0,000435234
3	1,154318E-05	0,8718344	4,025495E-05
4	2,608758E-07	0,8919935	2,559694E-06
5	5,895793E-09	0,9126186	4,304488E-08
6	1,332449E-10	0,9337207	3,732406E-10
7	3,011335E-12	0,9553108	1,150704E-11
8	6,805617E-14	0,9774	0
9	1,538069E-15	1	0
		Рно=	0,000478092
		Po=	0,999521908

$P_{У1}{}^{2} = P_O = 0{,}999521907516239$

Расчет эффективности декодера канала-3:

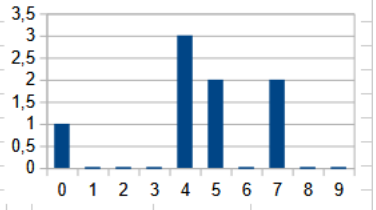
G=	1	0	0	0	1	1	0	1	0
	0	1	0	1	1	1	0	0	1
	0	0	1	0	1	0	1	1	0

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

p=	0,126
d*=	4
To=	3
Ти=	1
Po=	0,999266597

СПЕКТР КОДА

i	Ai
0	1
1	0
2	0
3	0
4	3
5	2
6	0
7	2
8	0
9	0
контроль	8



i	p^i	q^(n-i)	Apq
1	0,126	0,8328728	0
2	0,015876	0,852131	0
3	0,002000376	0,8718344	0
4	0,000252047	0,8919935	0,000674474
5	3,175797E-05	0,9126186	5,796583E-05
6	4,001504E-06	0,9337207	0
7	5,041895E-07	0,9553108	9,633154E-07
8	6,352788E-08	0,9774	0
9	8,004513E-09	1	0
		Рно=	0,000733403
		Po=	0,999266597

$P_{У1}{}^3 = P_O = 0{,}999266597016398$

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:

$$P_{У2}{}^i = 1 - v_i t / M_i^{Li}$$

Параметры M_i, L_i, v_i, t для трех средств аутентификации заданы для каждого варианта.

Результаты расчета эффективности средств аутентификации представлены в таблице:

Номер средства аутентификации	M_i	L_i	v_i	t	$P_{У2}{}^i$
1	98	8	555	50795	0,99999999668636
2	96	5	2750	50795	0,982868417055028
3	48	11	1875	50795	0,999999999969439

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,

K_c – коэффициент связности сети (среднее число связи для каждого узла),

$P_з$ – вероятность заражения при контакте узлов на одном шаге,

N – общее число узлов сети,

T – время действия эпидемии (во всех вариантах для всех вирусов – общее T=10).

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.

По результатам исследования рассчитывается эффективность защиты против каждого из вирусов:

$$P_{уз} = (N_{10}^З / N)$$

Расчет эффективности защиты против 1-го вируса

			i	NiБ	Ni3
Общее количество	500		0	20	480
Начальное заражение	20		1	60	440
Связность	8		2	170	330
Вер-ть заражения	0,26		3	404	96
				Рз=	0,19

$P_{уз}^1 = P_з = 0{,}192$

Расчет эффективности защиты против 2-го вируса

Общее количество	700		i	NiБ	Ni3
Начальное заражение	0		0	0	700
Связность	6		1	0	700
Вер-ть заражения	0,16		2	0	700
			3	0	700
				Рз=	1

$P_{уз}^{2} = P_з = 1$

Расчет эффективности защиты против 3-го вируса

Общее количество	940		i	NiБ	Ni3
Начальное заражение	24		0	24	916
Связность	7		1	54	886
Вер-ть заражения	0,18		2	119	821
			3	250	690
				Рз=	0,73

$P_{уз}^{3} = P_з = 0{,}734042553191489$

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:

	звено1	звено2	звено3	Ро	Рг
уровень1	0,99999617284	0,99952190752	0,99926659702	0,99926659702	0,99878503264
уровень2	0,99999999669	0,98286830774	0,99999999997	0,98286830774	0,98286830446
уровень3	0,192	1	0,734042553191	0,192	0,140936170213
Эффективность общая				0,99998984794	0,99998211906

2.5. Исследование зависимости эффективности всей подсистемы защиты против одиночного и группового воздействия при изменении параметра, указанного в варианте

На основе созданных выше моделей можно провести исследование зависимости показателей $P_о$ $P_г$, подставляя в модель разные исходные данные. Результаты исследования приведены в таблице.

Исследуемый параметр *No2*	$P_о$	$P_г$
5	0,99998984794	0,99998195562
10	0,99998984794	0,99998180475
15	0,99998984794	0,99998165808
20	0,99998984794	0,99998153236
25	0,99998984794	0,99998140244

На основе полученных данных можно построить график:

Вывод: изменение параметра защиты No2 уменьшает незначительно эффективность защиты.

КОНЕЦ