Автоматизация и моделирование в проектировании и управлении. 2023. № 4 (22). С. 37-44.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2023. № 4 (22). P. 37-44.

Научная статья
Статья в открытом доступе
УДК: 004.056.53
doi: 10.30987/2658-6436-2023-4-37-44

МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ ЭРГАТИЧЕСКОЙ СИСТЕМЫ КОНТРОЛЯ ИНФОРМАЦИОННОГО ОБМЕНА

Михаил Андреевич Бугорский
Краснодарское высшее военное училище, г. Краснодар, Россия
mr.bugorskey@mail.ru

Аннотация. *Целью данной статьи является создание имитационной модели, которая моделирует функционирование эргатической системы контроля информационного обмена и оценивает ее адекватность действующей системе. Так как в современном мире происходит быстрое развитие технологий и увеличивается объем обрабатываемой информации, то контроль за информационными ресурсами становится ключевым аспектом, что обуславливает актуальность данной статьи. Представлен анализ статистики утечек информации компании Info Watch за 2022 год, чтобы лучше понять масштаб проблемы. Рассмотрена подсистема контроля утечек изображений эргатической системы контроля информационного обмена. Рассмотрена модель, выполненная в имитационной среде CPN-Tools, которая позволит детально рассмотреть функционирование представленной системы. Эта модель позволит оценить, насколько эффективна система контроля информационного обмена в реальных условиях. На данном этапе предоставится возможность глубже понять как система работает и какие меры могут быть предприняты для улучшения ее функциональности. Данная статья представляет собой важный вклад в область контроля информационного обмена и безопасности данных, предлагая методологию и инструменты для анализа и улучшения эргатической системы контроля информационного обмена.*

Ключевые слова: утечка изображений, подсистема контроля утечек изображений, эргатическая системы контроля информационного обмена, DLP-система, автоматизированная система в защищенном исполнении

Для цитирования: Бугорский М.А. Модель функционирования эргатической системы контроля информационного обмена // Автоматизация и моделирование в проектировании и управлении. 2023. №4 (22). С. 37-44. doi: 10.30987/2658-6436-2023-4-37-44.

Original article
Open Access Article

MODEL OF OPERATING THE ERGATIC INFORMATION EXCHANGE CONTROL SYSTEM

Mikhail A. Bugorsky
Krasnodar Higher Military School, Krasnodar, Russia
mr.bugorskey@mail.ru

Abstract. *The aim of this article is to create a model that simulates the ergatic system operation for controlling information exchange and evaluates its adequacy to the current system. Since in the modern world there is rapid technology development and the volume of the processed information is increasing, the control over information resources is becoming a key aspect, which determines the article relevance. An analysis of Info Watch's 2022 information leak statistics is presented to better understand the scale of the problem. The subsystem for monitoring image leaks of the ergatic information exchange control systems is analysed. A model made in the CPN-Tools simulation environment is considered, which will allow examining in detail the presented system operation. This model will give the opportunity to evaluate how effective the information exchange control system is in real conditions. At this stage, it will be possible to gain deeper understanding of how the system works and what measures can be taken to improve its functionality. This article makes an important contribution to the field of information control and data security by proposing a methodology and tools for analysing and improving ergatic information exchange control systems.*

Keywords: image leakage, image leakage control subsystem, ergatic information exchange control system, DLP system, protected automated system

For citation: Bugorsky M.A. Model of Operating the Ergatic Information Exchange Control System. Automation and modeling in design and management, 2023, no. 4 (22). pp. 37-44. doi: 10.30987/2658-6436-2023-4-37-44.

Введение

В современном информационном обществе защита данных и информационная безопасность стали приоритетными задачами для организаций и пользователей. В этом контексте использование автоматизированных систем в защищенном исполнении (АСЗИ), способных эффективно решать проблемы защиты информации, становится все более актуальным. Одной из таких систем является Data Leakage Prevention система (DLP-система) Traffic Monitor. DLP-система контролирует информацию, циркулирующую в сегментах сети передачи данных и локальных персональных электронных вычислительных машинах (ПЭВМ) персонала организации, с целью предотвращения утечек конфиденциальной информации (КИ) и информации, составляющих коммерческую тайну (ИСКТ). Так как у названия DLP-системы нет нормативно-закрепленных понятий, будем называть ее системой контроля информационного обмена (КИО).

Необходимо отметить, что функции системы КИО являются инструментом, посредством которого операторы системы осуществляют свою деятельность в части предотвращения утечек информации. Взаимодействие системы КИО и операторами заключается в выявлении системой в открытом сегменте сети передачи данных (ОС СПД) и ПЭВМ пользователей КИ и ИСКТ.

Результат работы системы КИО проверяет дежурная смена экспертов и фиксирует количество ложноположительных срабатываний или ошибок I-го рода системы. Данные ошибки устраняются путем дообучения классификатора системы КИО промышленно-производственным персоналом.

Так как операторами и экспертами системы выполняется практическая деятельность, при которой проводится интеллектуализированная человекоинформационная связь с системой КИО, то полученный функциональный процесс образует эргатическую систему [6].

На основании вышесказанного, введем термин – эргатическая система контроля информационного обмена (ЭС КИО).

Эргатическая система контроля информационного обмена состоит из ряда подсистем, обеспечивающих предотвращение утечек всех видов информации, в том числе и графической – в виде изображений и графиков.

В данной статье мы рассмотрим модель функционирования подсистемы контроля утечек изображений (ПКУИ) ЭС КИО, а также ее возможности и перспективы в сфере информационной безопасности.

Актуальность

В современном мире в силу конфликтной военно-политической обстановки ужесточаются требования к защите информации, растет объем задач и, как следствие, растет объем обрабатываемой информации. В связи с этим, повышается сложность выполнения работ в данной области и проявляется нехватка человеческих ресурсов. Поэтому АСЗИ могут столкнуться с рядом сложных задач в части обработки больших объемов данных и расширения систем информационной безопасности, которые в свою очередь могут повлечь за собой повышенные риски утечки информации как по субъективным, так и объективным причинам.

По представленному в табл. 1 годовому отчету по отраслевому распределению утечек информации в России, подготовленному компанией InfoWatch [1], можно заметить, что доля утечек информации, произошедших в области высоких технологий составила 28,8 %.

Таблица 1

Отраслевое распределение утечек информации в России за 2022 год

Table 1

Industry distribution of information leaks in Russia for 2022

№ п/п	Наименование отрасли	Процент от общего количества утечек
1	Банки и финансы	7,3 %
2	Высокие технологии	28,8 %
3	Госорганы и силовые структуры	9,7 %
4	Другое/неопределено	15,5 %
5	Здравоохранение	1,7 %
6	Муниципальные учреждения	3,0 %
7	Образование	4,9 %

Подавляющее количество утечек информации, как представлено на рис. 1, относится к умышленным утечкам – 78,1 % от общего количества утечек за 2021 год и 79,5 % от общего количества утечек за 2022 год.

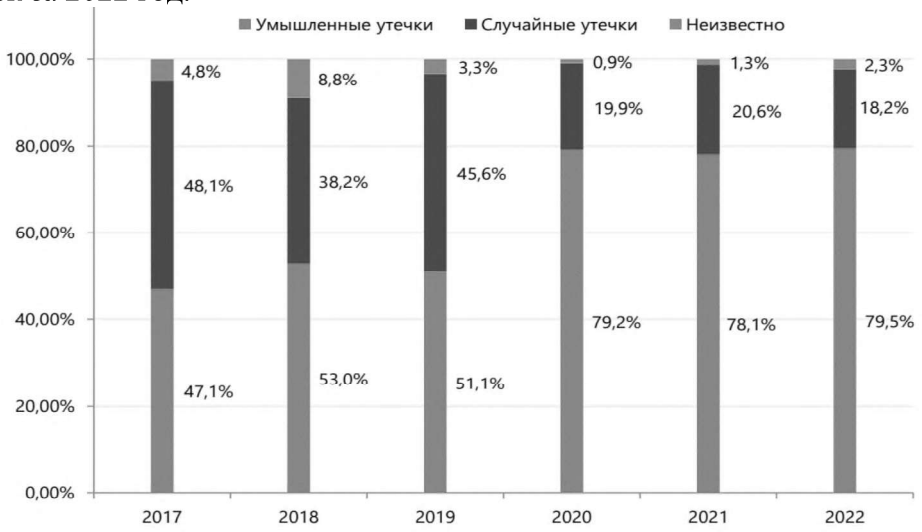

Рис. 1. Соотношение случайных и умышленных утечек информации среди нарушений внутреннего характера

Fig. 1. The ratio of accidental and intentional information leaks among internal violations

Перед ЭС КИО ставятся задачи по идентификации и классификации КИ и ИСКТ, контролю доступа к информации, мониторингу, обнаружению и предотвращению утечек КИ и ИСКТ, аудита и анализа данных и т.д. Каждая из задач выполняется соответствующей подсистемой ЭС КИО ВН.

Далее мы рассмотрим ПКУИ ЭС КИО, задачей которой является обнаружение изображений, содержащих КИ и ИСКТ на локальных ПЭВМ и предотвращение их утечек как случайных, так и умышленных по каналам ОС СПД организаций.

Модель ПКУИ ЭС КИО

Поэтапно опишем работу ПКУИ ЭС КИО (далее – подсистема):

Шаг 1. DLP-система сканирует трафик ОС СПД организации, а также локальные ПЭВМ пользователей на предмет наличия изображений.

Шаг 2. Обнаруженные изображения попадают в ПКУИ ЭС КИО, где с помощью искусственной нейронной сети (ИНС) определяется наличие в них КИ и/или ИСКТ.

Шаг 3. В случае наличия изображений, содержащих КИ и/или ИСКТ, они передаются на обработку операторам ПКУИ ЭС КИО для проверки точности работы ИНС, в противном случае, изображения покидают ПКУИ ЭС КИО.

Шаг 4. При подтверждении операторами наличия в изображении КИ и/или ИСКТ, оно передается на рассмотрение экспертам, в противном случае, изображение покидает ПКУИ ЭС КИО с отметкой об ошибке классификации ИНС (ошибка I-го рода).

Шаг 5. При подтверждении экспертами наличия в изображении КИ и/или ИСКТ, оно считается обработанным и передается установленным порядком в другие отделы организаций согласно установленных компетенций, в противном случае, изображение покидает ПКУИ ЭС КИО с отметкой об ошибке классификации ИНС и оператором (ошибка I-го рода).

Таким образом, работа ПКУИ ЭС КИО включает в себя три условных уровня проверки изображений, что позволяет предотвращать их утечку в случае наличия в них КИ и/или ИСКТ.

Для формализованного описания и анализа причинно-следственных связей рассматриваемой подсистемы будем использовать математический аппарат сетей Петри. Далее построим ее модель в виде графа *N*-схемы, который является двудольным ориентированным мультиграфом [7]. Он представляет собой совокупность позиций и переходов, представленных на рис. 2.

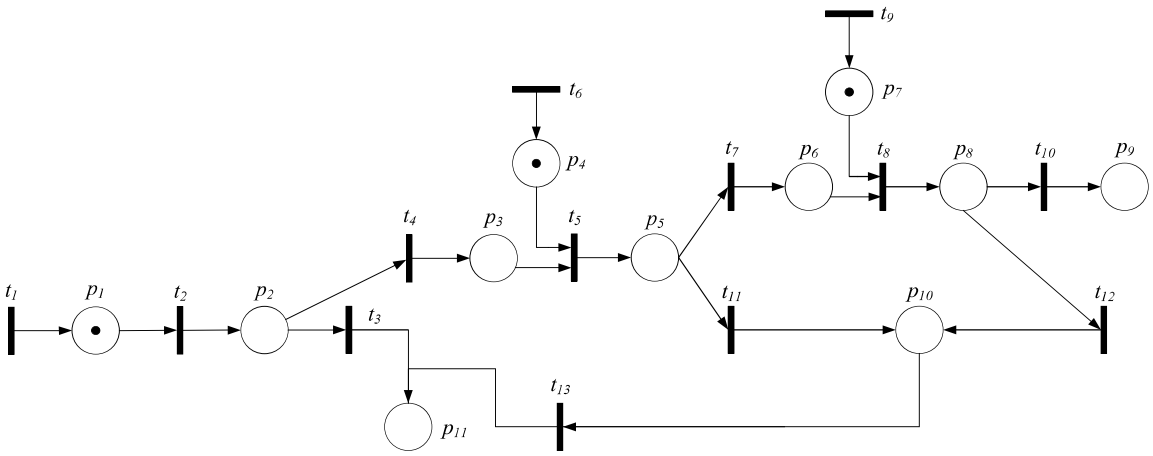

Рис. 2. Граф *N*-схемы ПКУИ ЭС КИО
Fig. 2. N-scheme graph of ILCS ES DLP

Сеть Петри состоит из множества позиций $P = \{p_q\}$, где $q = \{1, \dots, 11\}$ и является мощностью множества P; множества переходов $T = \{t_w\}$, где $w = \{1, \dots, 13\}$ и является мощностью множества T; входной функции I и выходной функции O [2].

Начальная маркировка (вектор разметки) имеет вид $\mu_0 = \{1,0,0,1,0,0,1,0,0,0,0\}$, где единицами обозначены фишки в позициях p_1, p_4 и p_7, обозначающие изображение, поступившее в ПКУИ ЭС КИО, ошибку I-го рода оператора и ошибку I-го рода эксперта соответственно.

В табл. 2 опишем функциональное назначение процессов ПКУИ ЭС КИО.

Таблица 2

Описание позиций и переходов процессов функционирования ПКУИ ЭС КИО

Table 2

Description of positions and transitions of ILCS ES DLP functioning processes

Описание позиций			Описание переходов	
p_1	ПКУИ ЭС КИО в готовности получить изображение от DLP-системы		t_1	Обнаружение изображения DLP-системой в ОС СПД или ПЭВМ организации
p_2	ИНС ПКУИ ЭС КИО определяет наличие КИ и/или ИСКТ в изображении		t_2	ПКУИ ЭС КИО принимает в обработку поступившее изображение
p_3	Оператор готов принять изображение от ИНС		t_3	Получение изображения, не содержащее КИ и/или ИСКТ от ИНС ПКУИ ЭС КИО
p_4	Ошибка I-го рода оператора		t_4	Получение изображения, содержащее КИ и/или ИСКТ от ИНС ПКУИ ЭС КИО
p_5	Оператор определяет наличие КИ и/или ИСКТ в изображении		t_5	Оператор принимает в обработку поступившее изображение
p_6	Эксперт готов принять изображение от ИНС		t_6	Вероятность ошибки I-го рода оператора
p_7	Ошибка I-го рода эксперта		t_7	Получение изображения, содержащее КИ и/или ИСКТ от оператора
p_8	Эксперт определяет наличие КИ и/или ИСКТ в изображении		t_8	Эксперт принимает в обработку поступившее изображение
p_9	Изображение, содержащее КИ и/или ИСКТ обработано		t_9	Вероятность ошибки I-го рода эксперта
p_{10}	Получение от оператора и/или эксперта неверно классифицированного изображения (ошибка I рода)		t_{10}	Получение изображения, содержащее КИ и/или ИСКТ от эксперта
p_{11}	Изображение, не содержащее КИ и/или ИСКТ обработано		t_{11}	Получение изображения, не содержащее КИ и/или ИСКТ от оператора
			t_{12}	Получение изображения, не содержащее КИ и/или ИСКТ от эксперта
			t_{13}	Получение изображения, не содержащее КИ и/или ИСКТ от дежурной смены

На основании вышеописанных позиций и переходов, создадим соответствующие им математические модели. Функция входных позиций перехода имеет вид:

$$D_1 = \{D_1(t_2), D_1(t_3), D_1(t_4), D_1(t_5), D_1(t_7), D_1(t_8), D_1(t_{10}), D_1(t_{11}), D_1(t_{12}), D_1(t_{13})\}, \quad (1)$$

где: $D_1(t_2) = \{p_1\}; D_1(t_3) = \{p_2\}; D_1(t_4) = \{p_2\}; D_1(t_5) = \{p_3, p_4\}; D_1(t_7) = \{p_5\}; D_1(t_8) = \{p_6, p_7\}; D_1(t_{10}) = \{p_8\}; D_1(t_{11}) = \{p_5\}; D_1(t_{12}) = \{p_8\}; D_1(t_{13}) = \{p_{10}\}.$ (2)

Функция выходных позиций перехода имеет вид:

$$D_2 = \{D_2(t_1), \dots, D_2(t_{13})\}, \quad (3)$$

где: $D_2(t_1) = \{p_1\}; D_2(t_2) = \{p_2\}; D_2(t_3) = \{p_{11}\}; D_2(t_4) = \{p_3\}; D_2(t_5) = \{p_5\}; D_2(t_6) = \{p_4\}; D_2(t_7) = \{p_6\}; D_2(t_8) = \{p_8\}; D_2(t_9) = \{p_7\}; D_2(t_{10}) = \{p_9\}; D_2(t_{11}) = \{p_{10}\}; D_2(t_{12}) = \{p_{10}\}; D_2(t_{13}) = \{p_{11}\}$ (4)

Для представления всех возможных связей между позициями и переходами сети Петри создадим матрицу инцидентности – табл. 3. С помощью нее предоставляется возможность определить, какие переходы могут активироваться из текущих позиций, что впоследствии поможет нам моделировать поведение системы и определить, какие переходы могут произойти при заданных условиях. Также мы сможем проанализировать свойства нашей сети Петри, такие как достижимость, активность и ограниченность.

Таблица 3

Матрица инцидентности сети Петри

Table 3

Petri net incidence matrix

	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}
t_1	1	0	0	0	0	0	0	0	0	0	0
t_2	-1	1	0	0	0	0	0	0	0	0	0
t_3	0	-1	0	0	0	0	0	0	0	0	1
t_4	0	-1	1	0	0	0	0	0	0	0	0
t_5	0	0	-1	-1	1	0	0	0	0	0	0
t_6	0	0	0	1	0	0	0	0	0	0	0
t_7	0	0	0	0	-1	1	0	0	0	0	0
t_8	0	0	0	0	0	-1	-1	1	0	0	0
t_9	0	0	0	0	0	0	1	0	0	0	0
t_{10}	0	0	0	0	0	0	0	-1	1	0	0
t_{11}	0	0	0	0	-1	0	0	0	0	1	0
t_{12}	0	0	0	0	0	0	0	-1	0	1	0
t_{13}	0	0	0	0	0	0	0	0	0	-1	1

В результате анализа матрицы инцидентности установлено, что данная сеть обладает свойствами:

1) достижимости, т.к. имеется хотя бы одна возможная траектория достижения маркера начальной позиции μ_0 в μ_q, где q = 11;

2) активности, т.к. возможно срабатывание любого перехода данной сети из множества $T = \{t_w\}$, где w = 13;

3) ограниченности, т.к. в процессе функционирования сети во всех позициях наблюдается число маркеров, не превышающее заданное.

Для оценки адекватности модели действующей системе, в среде CPN-Tools, была разработана имитационная модель ПКУИ ЭС КИО.

Для проверки адекватности необходимо сравнить статистические характеристики выборочной совокупности классифицированных изображений, полученные имитационной моделью, и характеристики генеральной совокупности классифицированных изображений. В качестве характеристик генеральной совокупности классифицированных изображений будем считать статистические данные, представленные специалистами организации.

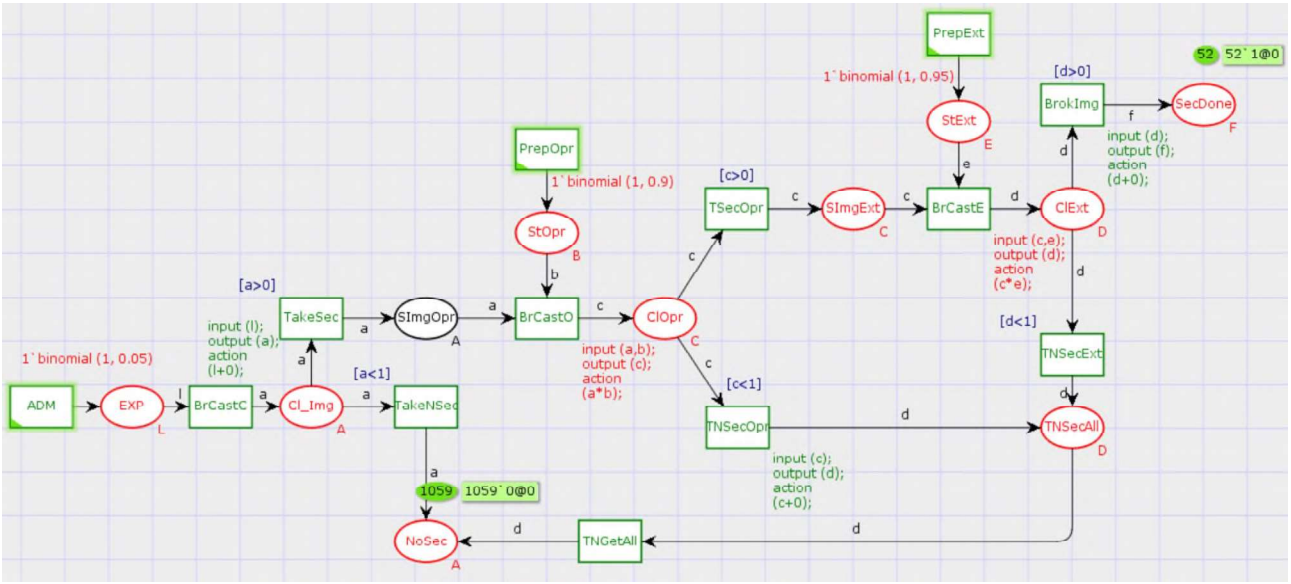

Рис. 3. Имитационная модель ПКУИ ЭС КИО
Fig. 3. Simulation model of ILCS ES DLP

В табл. 4 представлены вычисленные статистические данные выборочной и гипотетической генеральной совокупностей классифицированных изображений.

Таблица 4

Статистические данные выборочной и гипотетической генеральной совокупностей классифицированных изображений

Table 4

Statistics of sample and hypothetical populations of classified images

№ п/п	Наименование характеристики	Статистические данные выборочной совокупности классифицированных изображений, при количестве прогонов $n = 1111$ имитационной модели	Статистические данные генеральной совокупности классифицированных изображений
1	Дисперсия классифицированных изображений	$D_{\text{в}} = 0{,}044614$	$D_{\text{г}} = 0{,}049296$
2	Среднее квадратическое отклонение классифицированных изображений	$\sigma_{\text{в}} \approx 0{,}211$	$\sigma_{\text{г}} \approx 0{,}222$
3	Выборочная средняя классифицированных изображений	$\bar{x}_{\text{в}} = 0{,}0468$	$\bar{x}_{\text{г}} = 0{,}052$

Выборочная средняя классифицированных изображений $\bar{x}_{\text{в}}$ выборочной совокупности классифицированных изображений является несмещенной оценкой выборочной средней классифицированных изображений $\bar{x}_{\text{г}}$ генеральной совокупности классифицированных изображений, тогда:

$$M(\bar{X}_{\text{в}}) = a, \qquad (5)$$

где $\bar{X}_{\text{в}}$ – среднее арифметическое одинаково распределенных случайных величин выборочной совокупности классифицированных изображений.

Приняв во внимание, что каждая из величин $X_{\text{в}}$ имеет то же распределение, что и генеральная совокупность классифицированных изображений, заключаем, что числовые характеристики этих величин и генеральной совокупности классифицированных изображений одинаковы. В частности, математическое ожидание a каждой из величин равно математическому ожиданию признака $X_{\text{г}}$ генеральной совокупности классифицированных изображений:

$$M(X_{\text{г}}) = \bar{x}_{\text{г}} = a. \qquad (6)$$

Заменив в формуле (5) математическое ожидание a на $\bar{x}_{\text{г}}$, окончательно получим:

$$M(\bar{X}_{\text{в}}) = \bar{x}_{\text{г}}. \quad (7)$$

Далее воспользуемся критерием проверки нулевой гипотезы $H_0: a = a_0$. Учитывая, что выборочная средняя классифицированных изображений является несмещенной оценкой генеральной средней классифицированных изображений, нулевую гипотезу можно записать так:

$$M(\bar{X}_{\text{в}}) = a_0. \quad (8)$$

Таким образом, требуется проверить, что математическое ожидание выборочной средней классифицированных изображений равно гипотетической генеральной средней классифицированных изображений.

По формуле (9) найдем наблюдаемое значение критерия проверки нулевой гипотезы:

$$|U_{\text{набл}}| = (\bar{x}_{\text{в}} - a_0)\sqrt{n}/\sigma_{\text{в}}. \quad (9)$$

Подставив полученные значения в формулу (9), получим:

$$|U_{\text{набл}}| = (0{,}0468 - 0{,}052) \cdot 33{,}33/0{,}211 = 0{,}821.$$

По условию, конкурирующая гипотеза имеет вид $a \neq a_0$, поэтому критическая область – двусторонняя.

По формуле (10) найдем критическую точку $u_{\text{кр}}$:

$$\Phi(u_{\text{кр}}) = (1 - \beta)/2, \quad (10)$$

где β – уровень значимости, т.е. вероятность совершить ошибку I-го рода при отвержении верной нулевой гипотезы. Получим $\Phi(u_{\text{кр}}) = (1 - 0{,}01)/2 = 0{,}495$. По таблице функции Лапласа находим $u_{\text{кр}} = 2{,}58$.

Так как $|U_{\text{набл}}| < u_{\text{кр}}$ – нет оснований отвергнуть нулевую гипотезу, другими словами, выборочная и гипотетическая генеральная средние классифицированных изображений различаются незначимо. Таким образом, была доказана адекватность имитационной модели действующей системе.

Далее определим минимальное число прогонов имитационной модели. Так как случайные значения выходных характеристик имитационной модели некоррелированны и распределены одинаково, то число прогонов N имитационной модели, необходимое для того, чтобы истинное среднее x^0 классифицированных изображений с вероятностью $(1 - \gamma)$, где γ – надежность оценки результатов работы модели, лежало в интервале $\bar{y} \pm b$, определяется следующим образом [3]:

$$N = \frac{Z^2_{\gamma/2} \cdot \sigma_x^2}{b^2}, \quad (11)$$

где Z_x^2 – квантиль порядка $\gamma/2$ стандартного нормального распределения; σ_x^2 – дисперсия случайной величины x; b – доверительный интервал.

Так как значение дисперсии случайной величины до начала имитационного эксперимента и выборочное среднее уже определены, то вычислим предварительную оценку необходимого числа прогонов N, подставив значения в (11):

$$N = \frac{2{,}58^2 \cdot 0{,}044614}{0{,}01^2} \approx 2969,$$

где 2,58 – значение из таблицы интегральной функции Лапласа, т.к. квантиль порядка $\gamma/2 = \frac{0{,}99}{2} = 0495$.

Таким образом, для проверки точности имитационной модели, определяющую количество изображений, содержащих и не содержащих КИ и/или ИСКТ необходимо выполнить 2969 прогонов.

Заключение

Анализируя тенденции утечек информации в сфере информационной безопасности, требования, предъявляемые к АСЗИ и обеспечению информационной безопасности, и возможности ПКУИ ЭС КИО, мы можем сделать вывод о том, что представленные функции

системы являются мощным инструментом, обеспечивающим предотвращение утечек информации, в сфере информационной безопасности.

Проанализировав имитационную модель, представленную в статье, и доказав ее адекватность действующей системе и определив точность модели, мы предоставляем возможность разработать на ее основе новые модели и алгоритмы повышения эффективности функционирования ПКУИ ЭС КИО, например, таких как снижение ложноположительных и ложноотрицательных срабатываний системы и перераспределение ее ресурсов [5].

Список источников:

1. Аналитика отрасли информационной безопасности. [Электронный ресурс]. – URL: https://www.infowatch.ru/analytics/utechki-informatsii (дата обращения: 15.10.2023 г.)
2. Питерсон Дж. Теория сетей Петри и моделирование систем: Пер. с англ. – М.: Мир, 1984. – 264 с.
3. Надежность и эффективность в технике: Справочник: Н17 В 10 т. – Т. 3. Эффективность технических систем/Под общ. ред. В.Ф. Уткина, Ю.В. Крючкова. – М.: Машиностроение, 1988.– 328 с.
4. Гмурман В.Е. Теория вероятностей и математическая статистика: учебник для прикладного бакалавриата. – М.: Издательство Юрайт, 2017. – 479 с.
5. Бугорский М., Сизоненко А. Разработка модели повышения эффективности функционирования подсистемы контроля утечек изображений автоматизированной системы в защищенном исполнении за счет рационального перераспределения ресурсов // Вестник воронежского института высоких технологий. – URL: https://www.elibrary.ru/item.asp?id=50096595 (дата обращения: 15.10.2023).
6. ГОСТ 43.4.1-2011. Информационное обеспечение техники и операторской деятельности. Система «Человек – Информация»: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 13 декабря 2011 г. № 1243-ст: дата введения 2013-07-01 – URL: https://docs.cntd.ru/document/1200094359 (дата обращения: 15.10.2023).
7. Советов Б.Я., Яковлев С.А. Моделирование систем: Учеб. Для вузов – 3-е изд., перераб. и доп. – М.: высш. шк., 2001. – 343 с.

References:

1. Analysis of the Information Security Industry [Internet]. 2023 [cited 2023 Oct 15]. Available from: https://www.infowatch.ru/analytics/utechki-informatsii
2. Peterson J. Petri Net Theory and the Modelling of Systems. Moscow: Mir; 1984.
3. Utkina VF, Kryuchkova YuV, editors. Reliability and Efficiency in Technology: Directory: N17 in 10 Volumes. Volume 3, Efficiency of Technical Systems. Moscow: Mechanical Engineering; 1988.
4. Gmurman V.E. Probability Theory and Mathematical Statistics. Moscow: Yurayt; 2017.
5. Bugorsky M., Sizonenko A. Performance Improvement Model Subsystems of Image Leakage Control of Automated System in Protected Performance due to Rational Redistribution of Resources. The Bulletin of the Voronezh Institute of High Technologies [Internet]. 2022 [cited 2023 Oct 15]. Available from: https://www.elibrary.ru/item.asp?id=50096595
6. GOST 43.4.1-2011. Informational Ensuring of Equipment and Operational Activity. System "Man – Information" No. 1243-st. [Internet]. 2013 Jan 01 [cited 2023 Oct 15]. Available from: https://docs.cntd.ru/document/1200094359
7. Sovetov B.Ya., Yakovlev S.A. Systems Modelling. 3rd ed. Moscow: Vysshaya Shkola; 2001.

Информация об авторах:

Бугорский Михаил Андреевич
адъюнкт очной штатной адъюнктуры Краснодарского высшего военного училища

Information about the authors:

Bugorsky Mikhail Andreevich
Adjunct of the Full-Time Postgraduate Military Course at Krasnodar Higher Military School

Статья поступила в редакцию 26.10.2023; одобрена после рецензирования 15.11.2023; принята к публикации 16.11.2023.

The article was submitted 26.10.2023; approved after reviewing 15.11.2023; accepted for publication 16.11.2023.

Рецензент – Рытов М.Ю., кандидат технических наук, доцент, Брянский государственный технический университет.

Reviewer – Rytov M.Yu., Candidate of Technical Sciences, Associate Professor, Bryansk State Technical University.