УДК 004.31:681.513.6+ 004.891.3 Вестник УрФО № 2(44) / 2022, с. 37–42

Егорова А.О., Тищенко Е.Н.

DOI: 10.14529/secur220205

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АДАПТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

В статье приводится математическая модель системы защиты информации от утечки по техническим каналам с адаптивным управлением. Модель представляет собой комбинацию моделей нескольких подсистем. Предложенная модель описывает принципы функционирования подсистем генерирования псевдослучайных последовательностей для задач системы, машинного обучения, защиты от утечки информации, оценки защищенности информации. Приведённая математическая модель в дальнейшем может быть использована для построения аппаратно-программного комплекса для защиты информации от утечки по техническим каналам.

Ключевые слова: *технические каналы утечки информации, математическая модель, машинное обучение, защита информации, маскирующий сигнал, речеподобный шумовой сигнал.*

Egorova A.O., Tishchenko E.N.

MATHEMATICAL MODEL OF ADAPTIVE SYSTEM OF INFORMATION SECURITY FROM LEAKAGE THROUGH TECHNICAL CHANNELS

The article presents a mathematical model of the information security system against leakage through technical channels with adaptive control. The model is a combination of models of several subsystems. The proposed model describes the principles of functioning of subsystems for generating pseudo-random sequences for system tasks, machine learning,

information leakage protection, and information security assessment. The above mathematical model can be used later to build a hardware-software complex for the security of information from leakage through technical channels.

Keywords: *technical channels of information leakage, mathematical model, machine learning, information security, masking signal, speech-like noise signal.*

Целью данной работы является разработка математической модели адаптивной системы защиты информации от утечки по техническим каналам. Разрабатываемая модель представляет собой основу для проектирования систем защиты информации от утечки по техническим каналам с адаптивным управлением.

Защита информации от утечки по техническим каналам с помощью средств активной технической защиты производится путем блокирования электромагнитных, электрических и акустических сигналов, препятствуя распространению информативного сигнала за пределы помещений, в которых циркулирует информация. Построение математической модели адаптивной системы защиты информации от утечки по техническим каналам начинается описания структуры. Компоненты модели:

1. Модель генератора случайных чисел – генерирует выделенную частоту из диапазона, определяемого исходя из выбранного канала утечки информации.

2. Модель блокирования канала утечки информации – определяет требования к задаваемой мощности шумового сигнала.

3. Модель машинного обучения – задаёт алгоритм и параметры обучения.

4. Модель системы оценки эффективности защиты информации – проводит анализ функционирования системы защиты информации на соответствие критериям защищенности.

Следует рассмотреть вышеуказанные модели более детально.

Для обучения разрабатываемой системы следует использовать множества X объектов и Y ответов. Тогда следует предположить, что существует функциональная зависимость:

$$F : X \to Y \qquad (1)$$

Зависимость между объектами и ответами неизвестны, но известна обучающая выборка:

$$S = \{(x_i, y_{xi} = F(x_i) \in X \times Y) | i=1, \ldots, l\} \qquad (2)$$

Задача обучения — найти аппроксимирующую функцию $a_S : X \to Y$ такой, что

$$\forall x \in X \quad a_S(x) \approx F(x) \qquad (3)$$

Для решения задачи построения функции $a_S : X \to Y$ по обучающей выборке S выбирается некоторая модель обучения. Структура модели представлена как взаимосвязь двух компонент:

1. Предсказательная модель:

$$a : X \times W \to Y \qquad (4)$$

где W – множество параметров.

Для нахождения искомой функции a_S используется следующая зависимость:

$$a_S(x) = a(x,w) \qquad (5)$$

Проектируемая модель должна решать задачи регрессии, поскольку она позволяет прогнозировать значения множества ответов Y. Для этого следует использовать линейную предсказательную модель. В линейной предсказательной модели множество W параметров имеет вид R^n, где n – число признаков объектов, т.е. каждый параметр w представляет собой вектор действительных чисел $w = (w_1, w_2, \ldots, w_n)$, и $Y = R$, и

$$a(x, w) = \langle x, w \rangle \stackrel{\text{def}}{=} \sum_{i=1}^{n} x^i w_i \qquad (6)$$

где $\langle x, w \rangle$ - скалярное произведение x и w.

2. Алгоритм обучения – алгоритм поиска такого значения w, для которого функция a_S, определяемая соотношением (5), обладает некоторыми свойствами оптимальности. Для точного описания свойств оптимальности алгоритмов обучения используется понятие функции потерь, которая сопоставляет паре (a_S, x), где $x \in X$, число $\mathcal{L}(a_S, x)$, выражающее величину ошибки аппроксимации a_S на объекте $x \in X$. Задач регрессии функция потерь имеет вид:

$$\mathcal{L}(a_S, x) = (a_S(x) - f(x))^2 \qquad (7)$$

Функционал эмпирического риска аппроксимации a_S, используемый в описаниях свойств оптимальности алгоритмов обучения вычисляется следующим образом:

$$Q(a_S) = \frac{1}{l} \sum_i^l \mathcal{L}(a_S, S) \qquad (8)$$

Таким образом, одно из свойств оптимальности алгоритма обучения по обучающей выборке S заключается в том, что значение параметра $w \in W$, определяющее наилучшую аппроксимацию a_S, должно удовлетворять соотношению

$$w = \arg\min_{w \in W} Q(a_S) \qquad (9)$$

Исходя из вышеизложенного, решение

задачи машинного обучения сводится к нахождению такого параметра $w \in W$, который минимизирует риск $Q(a_s)$.

Первой задачей при построении модели генератора случайных чисел стоит выбор типа генератора. Разновидности генераторов случайных чисел по способу получения чисел приведён на рисунке 1.

Рис.1. Классификация генераторов случайных чисел

Оптимальным выбором для разрабатываемой системы являются алгоритмические генераторы случайных чисел, поскольку они отличаются малой ресурсоемкостью и быстродействием. Однако, при оценке эффективности системы защиты информации следует учитывать тот факт, что алгоритмические генераторы позволяют получить только псевдослучайные числа [1].

Наиболее часто используемым алгоритмическим методом генерации псевдослучайных чисел является линейный конгруэнтный метод. Его базовое преимущество заключается в простоте реализации, что позволяет минимизировать затраты вычислительных ресурсов. Вычисление последовательности производится по формуле:

$$r_{i+1} = \mathrm{mod}(k \cdot r_i + b, M) \qquad (10)$$

В формуле (10) k – множитель, b – приращение, M – модуль, r_i – предшествующий элемент последовательности, где $k \in [0; M)$, $b \in [0; M)$ $r_i \in [0; M)$ и $M \in (0; +\infty)$. При этом b и M взаимно простые. Оптимальным выбором значения модуля является $M = 2^N - 1$ при использовании алгоритма в двоичных вычислительных системах [2].

Моделирование активной защиты информации от утечки по техническим каналам производится на основании схемы, приведённой на рисунке 2 [3, С. 168-175].

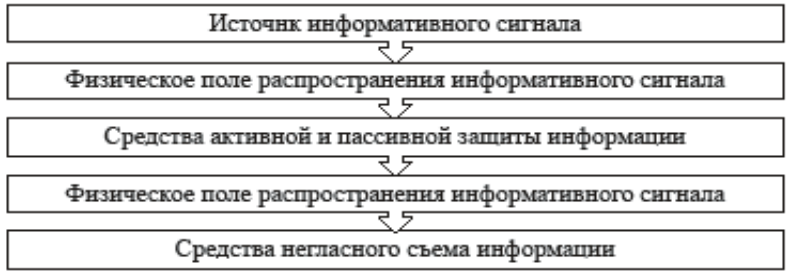

Рис. 2. Структура технического канала утечки информации

Технические каналы утечки информации по физической природе носителя делятся на:

– оптические;

– радиоэлектронные;

– акустические;

– материально-вещественные [4].

Из вышеприведённых каналов средства активной защиты применяются для акустических и радиоэлектронных каналов. Следовательно, алгоритм вычисления мощности должен учитывать модели указанных каналов.

Акустические каналы утечки информации представляют собой технические каналы, в которых полезный сигнал представляет собой акустический сигнал. Акустический сигнал представляет собой возмущения упругой среды, проявляющиеся в возникновении акустических колебаний различной формы и длительности, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины [5]. Классификация акустических каналов по физической природе приведена на рисунке 3.

Для блокирования приведённых выше каналов утечки информации используют средства активной акустической маскировки, которая снижает отношение сигнал/шум на входе технического средства разведки за счет увеличения уровня шума (помехи). Виброакустическая маскировка эффективно используется для защиты речевой информации от утечки по прямому акустическому, виброа-

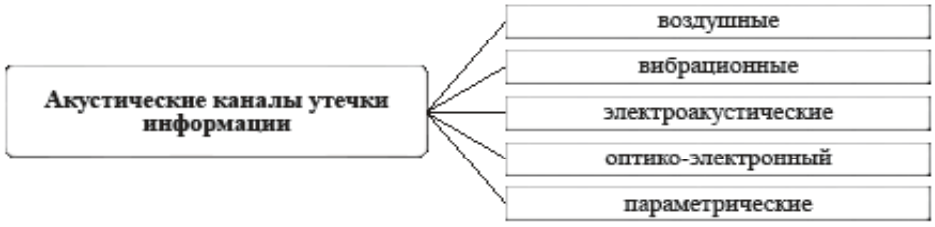

Рис. 3. Классификация акустических каналов утечки информации

кустическому и оптико-электронному каналам утечки информации. Для формирования акустических помех применяются специальные генераторы, к выходам которых подключены звуковые колонки (громкоговорители) или вибрационные излучатели (вибродатчики) Большую группу генераторов шума составляют устройства, принцип действия которых основан на усилении колебаний первичных источников шумов. В качестве источников шумовых колебаний используются электровакуумные, газоразрядные, полупроводниковые и другие электронные приборы, и элементы. Временной случайный процесс, близкий по своим свойствам к шумовым колебаниям, может быть получен и с помощью цифровых генераторов шума, формирующих последовательности двоичных символов, называемые псевдослучайными.

Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС - линейное зашумление [6].

Механизм действия устройств зашумления в основе схожий для всех каналов утечки информации, где используются подобные средства. Сформированный генератором шумовой сигнал направляется на устройства вывода (динамики, антенны и т.д.). При достаточной мощности излучения и соответствия блокируемому полезному сигналу (частотные диапазоны разных каналов передачи информации различаются) за пределами контролируемой зоны на техническое средство разведки поступает шумовой сигнал, в котором становится невозможно выделить полезный сигнал.

Так, для защиты от утечки информации озвучиваемой на объекте информатизации, в качестве маскирующего шума может быть использован речеподобный шумовой сигнал. Речеподобный шум создают из исходного речевого сигнала путем его фазовой модуляции шумовым сигналом, что приводит к разрушению формантной структуры исходного речевого сигнала. Формальная запись представлена ниже.

$$S(t) = \sum_{p=1}^{N} U_p(t) \sin\left[2\pi\rho \int_0^1 F_0(\tau)\, d\tau + \right.$$
$$\left. + \Phi_\rho(t)\right] + r(t),\ S_{\text{РПП}}(t) = \sum_{j=1}^{6} \sum_{p=1}^{N} U_{pj}(t)$$
$$\sin\left[2\pi\rho \int_0^{t-t_j} F_0(\tau)\, d\tau + \Phi_{\rho j}(t)\right] +$$
$$+ \sum_{j=1}^{6} r_j(t) \qquad (11)$$

где $S(t)$ – речевой сигнал, $S_{\text{РПП}}(t)$ – речеподобный шумовой сигнал, $F_0(\tau)$ – мгновенная частота основного тона звука, $U_p(t)$ – амплитуда p-ой гармонической составляющей звука, N – фаза -ой гармонической составляющей звука, $r(t)$– число энергетически значимых гармонических составляющих звука, $t \in [0; T]$, $\tau \in [0; t]$, T – шумовая составляющая звука, j – время анализа звука; t_j – количество каналов в генераторе речеподобной помехи; – интервалы задержки исходного сигнала в каналах генератора [7].

В системах зашумления в электрическом и магнитном полях используются помехи типа «белый шум» – стационарный шум, спектральные составляющие которого равномерно распределены по всему диапазону задействованных частот.

Базовым методом оценки эффективности защиты информации от утечки по техническим каналам является определение уровня сигнал/шум для рассматриваемого объекта информатизации. Уровень сигнала/шум в месте размещения датчика в i-го частотного интервала:

$$\Delta = L_{ci} - L_{ши} \qquad (12)$$

Для дополнительной оценки защищенности речевой информации от утечки по техническим каналам применяется метод оценки разборчивости речи [8], которая заключается в следующем:

1. Разделение частотного диапазона на определенное число смежных полос (октавных полос).

2. Определение формантного параметра

спектра речевого сигнала в октавной полосе ΔA_i

$$\Delta A_i = \begin{cases} 200f^{0,43} - 0,37, \text{если } f \le 1000 \text{ Гц} \\ 1,37 - \frac{1000}{f^{0,69}}, \text{если } f > 1000 \text{ Гц} \end{cases} \quad (13)$$

3. Определение эффективного уровня ощущений формант Q_i для каждой средней частоты f_i каждой полосы.

$$Q_i = \Delta - \Delta A_i \quad (14)$$

4. Расчет коэффициента восприятия формант для каждой октавной полосы

$$P_i = \begin{cases} \frac{0,78+5,46 \cdot e^{\left[-4,3 \cdot 10^{-3} \cdot (27,3-|Q_i|)^2\right]}}{1+10^{0,1 \cdot |Q_i|}}, \text{если } Q_i \le 0 \\ 1 - \frac{0,78+5,46 \cdot e^{\left[-4,3 \cdot 10^{-3} \cdot (27,3-|Q_i|)^2\right]}}{1+10^{0,1 \cdot |Q_i|}}, \text{если } Q_i > 0 \end{cases} \quad (15)$$

5. Расчет формантной разборчивости

$$R = \sum_{i=1}^{n} P_i k_i \quad (16)$$

где $k_i = \begin{cases} 2,57 \cdot 10^{-8} \cdot f^{2,4}, \text{если } 100 < \\ 1 - 1,047 \cdot e^{-10^{-4} \cdot f^{1,18}}, \text{если } 400 < \end{cases}$

$< f \le 400$ Гц
$< f \le 10000$ Гц – весовой коэффициент.

6. Вычисление словесной разборчивости

$$W = \begin{cases} 1,54 \cdot R^{0,25} \cdot [1 - e^{-11R}], \text{если } \langle R \rangle < 0,15 \\ 1 - e^{-\frac{11R}{1+0,7R}}, \text{если } \langle R \rangle \ge 0,15 \end{cases} \quad (17)$$

Рассмотрим элементарный электрический излучатель (диполь Герца) в сферической системе координат (рисунок 3)

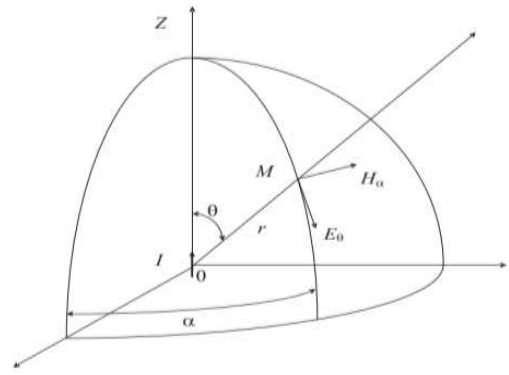

Рис. 3. Элементарный электрический диполь в сферической системе координат

Амплитуда напряжённости электрической E_m и магнитной H_m составляющих электромагнитного поля, которые измеряются с использованием электрических и магнитных антенн имеют вид:

$$E_m = \frac{klI_m}{4\pi\omega\varepsilon r} \sqrt{\left(\frac{3}{k^2r^2} + \frac{5}{r^2}\right)\cos^2(\vartheta) + k^2\sin^2(\vartheta) + \frac{1}{k^2r^2} - \frac{1}{r^2}} \quad (18)$$

$$H_m = \frac{klI_m}{4\pi r} \sqrt{\frac{1}{k^2r^2} + 1} \cdot \sin(\vartheta) \quad (19)$$

Параметры электрического диполя, стоящие перед корнем в уравнениях для E_m и H_m, могут быть определены из измерений электрической и магнитной составляющей электромагнитного поля. Следовательно, оценка защищённости может быть сведена к численному решению уравнений вида $E_m = E_n$ и $H_m = H_n$, где величины E_n и H_n определяются нормативно-методическими документами [9].

Таким образом, в данной работе описана модель обучения адаптивной системы на основе базовой модели машинного обучения. В качестве алгоритма обучения выбран метод восстановления регрессии – метод наименьших квадратов. Также для решения поставленных задач линейный конгруэнтный метод генерации псевдослучайной последовательности выбран как оптимальный. Защита информации от утечки по техническим каналам в части касающейся разрабатываемой модели в общем виде представляет собой применение устройств пространственного и линейного зашумления, шумовой сигнал для которых будет сформирован в виде речеподобного шума для акустических сигналов и в виде белого шума – для электрических и магнитных сигналов.

Литература

1. Генераторы случайных чисел [Электронный ресурс]. — Режим доступа: https://intellect.icu/generatory-sluchajnykh-chisel-5256.

2. Генераторы случайных чисел [Электронный ресурс]. — Режим доступа: http://stratum.ac.ru/education/textbooks/modelir/lection22.html.

3. Реализация ESG-принципов в стратегии устойчивого развития экономики России: монография / Н.Г. Вовченко и др.; под. ред. д.э.н., проф. Е.Н. Макаренко, д.геогр.н., проф. С.В. Бердникова. – Ростов-на-Дону: Издательскополиграфический комплекс Рост. гос. экон. ун-та (РИНХ), 2022. – 508 с.

4. Общие вопросы технической защиты информации [Электронный ресурс]. — Режим доступа: https://intuit.ru/studies/courses/2291/591/lecture/12696?page=1.

5. Технические каналы утечки акустической (речевой) информации Хорев А.А. Специальная техника. 1998. № 1. С. 50.

6. Хорев А.А. Способы и средства зашиты информации. - М.: МО РФ, 2000. - 316 с.

7. Моисеева, М. В. Система защиты информации от утечки по акустическим каналам на основе речеподобной помехи / М. В. Моисеева, А. В. Фурсова // Инновационные процессы в научной среде: Материалы Международной (заочной) научно-практической конференции, Прага, 16 июня 2021 года / под общей редакцией А.И. Вострецова. – Нефтекамск: Научно-издательский центр «Мир науки» (ИП Вострецов Александр Ильич), 2021. – С. 78-84.

8. Рева, И. Л. Реализация оптимальной помехи при защите речевой информации от утечки по акустическому и виброакустическому каналам / И. Л. Рева, В. А. Трушин, А. В. Иванов // Научный вестник Новосибирского государственного технического университета. – 2011. – № 4(45). – С. 140-145.

9. Носов, Л. С. Оценка защищённости СВТ путём моделирования канала ПЭМИН / Л. С. Носов // Математические структуры и моделирование. – 2014. – № 4(32). – С. 254-257

References

1. Generatory sluchajnyh chisel [Jelektronnyj resurs]. — Rezhim dostupa: https://intellect.icu/generatory-sluchajnykh-chisel-5256.

2. Generatory sluchajnyh chisel [Jelektronnyj resurs]. — Rezhim dostupa: http://stratum.ac.ru/education/textbooks/modelir/lection22.html.

3. Realizacija ESG-principov v strategii ustojchivogo razvitija jekonomiki Rossii: monografija / N.G. Vovchenko i dr.; pod. red. d.je.n., prof. E.N. Makarenko, d.geogr.n., prof. S.V. Berdnikova. – Rostov-na-Donu: Izdatel'sko poligraficheskij kompleks Rost. gos. jekon. un-ta (RINH), 2022. – 508 s.

4. Obshhie voprosy tehnicheskoj zashhity informacii [Jelektronnyj resurs]. — Rezhim dostupa: https://intuit.ru/studies/courses/2291/591/lecture/12696?page=1.

5. Tehnicheskie kanaly utechki akusticheskoj (rechevoj) informacii Horev A.A. Special'naja tehnika. 1998. № 1. S. 50.

6. Horev A.A. Sposoby i sredstva zashity informacii. - M.: MO RF, 2000. - 316 s.

7. Moiseeva, M. V. Sistema zashhity informacii ot utechki po akusticheskim kanalam na osnove rechepodobnoj pomehi / M. V. Moiseeva, A. V. Fursova // Innovacionnye processy v nauchnoj srede: Materialy Mezhdunarodnoj (zaochnoj) nauchno-prakticheskoj konferencii, Praga, 16 ijunja 2021 goda / pod obshhej redakciej A.I. Vostrecova. – Neftekamsk: Nauchno-izdatel'skij centr "Mir nauki" (IP Vostrecov Aleksandr Il'ich), 2021. – S. 78-84.

8. Reva, I. L. Realizacija optimal'noj pomehi pri zashhite rechevoj informacii ot utechki po akusticheskomu i vibroakusticheskomu kanalam / I. L. Reva, V. A. Trushin, A. V. Ivanov // Nauchnyj vestnik Novosibirskogo gosudarstvennogo tehnicheskogo universiteta. – 2011. – № 4(45). – S. 140-145.

9. Nosov, L. S. Ocenka zashhishhjonnosti SVT putjom modelirovanija kanala PJeMIN / L. S. Nosov // Matematicheskie struktury i modelirovanie. – 2014. – № 4(32). – S. 254-257.

ЕГОРОВА Анастасия Олеговна, аспирант кафедры Информационных технологий и защиты информации, Ростовский государственный экономический университет (РИНХ). 344002, г. Ростов-на-Дону, ул. Б. Садовая, 69. E-mail: anastasya-olegovna.kalita@yandex.ru.

ТИЩЕНКО Евгений Николаевич, доктор экономический наук, профессор, декан факультета Компьютерных технологий и информационной безопасности, Ростовский государственный экономический университет (РИНХ). 344002, г. Ростов-на-Дону, ул. Б. Садовая, 69. E-mail: celt@inbox.ru.

EGOROVA Anastasia Olegovna, Postgraduate Student, Department of Information Technologies and Information Protection, Rostov State University of Economics. 344002, Rostov-on-Don, st. B. Sadovaya, 69. E-mail: anastasya-olegovna.kalita@yandex.ru.

TISCHENKO Evgeny Nikolaevich, Doctor of Economics, Professor, Dean of the Faculty of Computer Technologies and Information Security, Rostov State University of Economics. 344002, Rostov-on-Don, st. B. Sadovaya, 69. E-mail: celt@inbox.ru.