УДК: 004.771 DOI: 10.53816/23061456_2022_1–2_72

МОДЕЛЬ ПРОЦЕССА РАСПОЗНАВАНИЯ ЭЛЕМЕНТОВ КОРПОРАТИВНОЙ СИСТЕМЫ ТЕЛЕКОММУНИКАЦИОННОЙ СВЯЗИ СРЕДСТВАМИ ТЕХНИЧЕСКОЙ КОМПЬЮТЕРНОЙ РАЗВЕДКИ

MODEL OF RECOGNITION PROCESS OF CORPORATE TELECOMMUNICATION SYSTEM ELEMENTS BY TECHNICAL COMPUTER INTELLIGENCE

Д-р техн. наук О.М. Лепешкин, А.С. Пермяков

D.Sc. O.M. Lepeshkin, A.S. Permyakov

Военная академия связи им. С.М. Буденного

В статье представлена модель распознавания элементов корпоративной системы телекоммуникационной связи (СТС) средствами технической компьютерной разведки (ТКР), предназначенная для исследования процесса функционирования СТС, выявления демаскирующих признаков (ДМП) ее элементов в статическом и динамическом режимах, определения информативности ДМП относительно элементов других систем связи, функционирующих в том же фрагменте сети связи общего пользования (ССОП), вычисления коэффициентов контраста элементов СТС, а также вероятности ее вскрытия средствами ТКР. В качестве метрики для контрастности выбрано взвешенное евклидово расстояние, а вероятность распознавания элементов системы связи за время квазистационарного состояния, вычисляется после проведения автоматического кластер-анализа элементов систем связи фрагмента ССОП.
Ключевые слова: система телекоммуникационной связи, техническая компьютерная разведка, вероятность вскрытия, модель системы связи.

The article presents a model for recognizing elements of a corporate telecommunication system (CTS) by means of technical computer intelligence (TCI), designed to study the process of functioning of a CTS, identify unmasking features (IUF) of its elements in static and dynamic modes, determine the information content of a IUF relative to elements of other communication systems operating in the same fragment of the public communications network (PCN), calculating the contrast coefficients of the CTS elements, as well as the probability of its opening by means of TCI. The weighted Euclidean distance was chosen as a metric for contrast, and the probability of recognizing the elements of the communication system during the quasi-stationary state is calculated after the automatic cluster analysis of the elements of the communication systems of the PCN fragment.
Keywords: telecommunication communication system, technical computer intelligence, opening probability, communication system model.

Инфокоммуникационное пространство стало практически безальтернативной средой для обмена информацией между людьми, организациями, государственными учреждениями, а также транснациональными компаниями. По заверениям операторов связи, предоставляемые телекоммуникационные услуги надежны и безопасны. Возникающие угрозы деструктивных

программно-аппаратных воздействий скрываются, противодействие им остается в зоне ответственности пользователей услуг, а также организаций, специализирующихся на обеспечении безопасности информации. В то же время ущерб, возникающий в результате деятельности технической компьютерной разведки (ТКР), может носить не только репутационный и финансовый характер, но и быть вполне реальным, вплоть до физического уничтожения объектов информационной инфраструктуры [1].

Сеть связи общего пользования (ССОП), объединяющая разнородных и разрозненных операторов телекоммуникационных услуг, является технической основой для построения распределенных систем связи различного масштаба и уровня. Особенностью ее архитектуры является наличие трафикообменных центров, через которые проходит абсолютное большинство передаваемых дейтаграмм между отправителями и получателями данных. Доступ к указанным узлам сети со стороны ТКР обеспечивает ей полную картину происходящего в инфокоммуникационном пространстве, включающую информацию о конечных и транзитных пунктах передачи информации, задействованном оборудовании и его конфигурации, используемых протоколах, а также интенсивности информационного обмена. Целью нарушителей может стать как сама передаваемая информация, так и расположение элементов сети.

Организовать противодействие целенаправленным атакам достаточно сложно и дорого, особенно учитывая тот факт, что регулярно появляются новые, ранее не известные, так называемые, уязвимости нулевого дня. Одним из направлений защиты элементов распределенной корпоративной СТС является скрытие ее элементов среди элементов других сетей связи, функционирующих в том же фрагменте ССОП.

Предметом проводимого исследования является разведзащищенность корпоративной СТС, заключающаяся в ее способности противостоять всем видам разведки, сохранении в тайне ее структуры и порядка функционирования, в том числе мест расположения узлов связи, других элементов системы и режимов работы средств связи [2].

Известные модели инфокоммуникационных систем [3–5], включающие возможности реконфигурации, генерирования ложного трафика, не учитывают окружающее инфокоммуникационное пространство защищаемой сети, а также степень отличия от него элементов СТС.

Моделируемая корпоративная СТС представляет собой сложную территориально распределенную систему, в которой, в зависимости от назначения элементов и связей между ними, используются различные протоколы передачи данных и способы установления соединений. Исследуемая система строится поверх существующей глобальной информационно телекоммуникационной сети Интернет, в следствие чего интегрирована в ССОП единой сети электросвязи Российской Федерации и имеет подключения к сетям связи иностранных государств (рис. 1).

Процесс ведения ТКР включает обнаружение объектов (элементов СТС) и их последующее распознавание по характерным ДМП, в случае контакта средства разведки и элемента СТС [6].

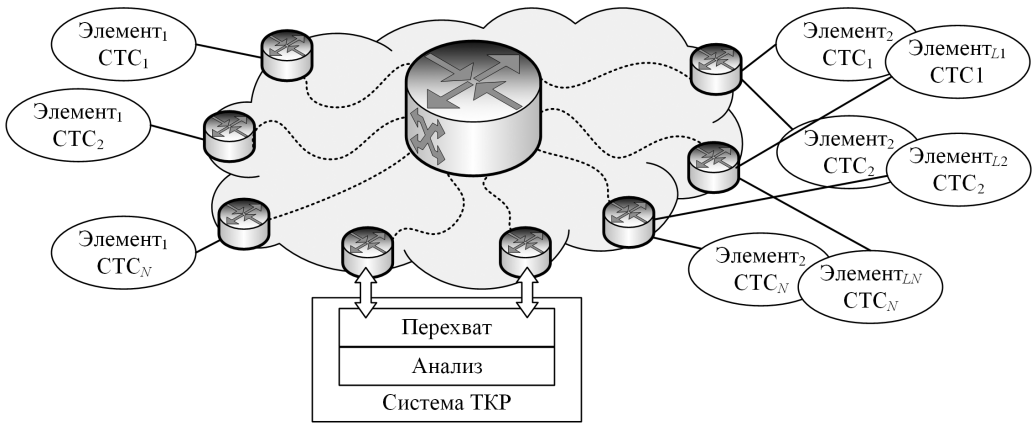

Рис. 1. Схема процесса сетевого взаимодействия

Под обнаружением понимается выделение на окружающем фоне каких-либо объектов, отличных по своим характеристикам от фона, которые подвергаются дальнейшему анализу. Различие характеристик объекта и фона называется контрастом. Чем больше контраст, тем выше вероятность того, что объект будет выделен и обнаружен. Под контрастностью в инфокоммуникационном пространстве понимается степень отличия набора значений параметров элемента сети от наборов подобных параметров других элементов, функционирующих в том районе ССОП.

Распознавание заключается в отнесении обнаруженного объекта к одному из известных классов по определенным признакам. У объекта может быть достаточно большое число признаков, однако при распознавании используют их определенный набор. Под признаком понимается любое свойство объекта, поддающееся количественному или качественному описанию [7].

Элементы корпоративной СТС характеризуются изменяющимися во времени ДМП, по которым ТКР может выполнить их распознавание. Разделим их на три группы:

$$\Theta = \Theta(P_1, P_2, P_3, t),$$

где Θ — условное обозначение объекта распознавания; P_1 — признаки, характеризующие сетевые параметры объекта; P_2 — пространственные признаки, характеризующие координаты объекта в пространстве; P_3 — признаки, характеризующие наличие определенных связей между объектами и их элементами; t — время.

При распознавании объектов одновременно используются K признаков и объект распознавания геометрически представляется точкой в K-мерном пространстве признаков. При большом K возникают сложности с классификацией, многие из признаков могут быть малоинформативны, поэтому целесообразно сократить их количество и добиться, чтобы они были не коррелированы.

Если с течением времени ДМП элементов системы связи остаются неизменными, вероятность вскрытия ее структуры возрастает многократно.

ДМП элементов СТС с точки зрения изменчивости подразделяются на две группы: изменяемые и неизменяемые. Каждый ДМП имеет свою контрастность относительно ДМП элементов других сетей связи. Наиболее информативные ДМП, доступные для обнаружения средствами ТКР, представлены в таблице.

При моделировании распознавания необходимо рассматривать проявление ДМП системы и ее элементов как в статическом состоянии, так и в динамике, выявляя ДМП процесса функционирования, связанного с информационным обменом. В статическом состоянии средства ТКР могут выявлять ДМП путем сканирования сети, а в динамическом состоянии путем перехвата и анализа передаваемых дейтаграмм.

Таким образом, для определения показателей разведзащищенности требуется вычислить контрастность ДМП элементов СТС относительно ДМП элементов других систем связи в одном фрагменте ССОП в статическом режиме и ДМП передаваемых дейтаграмм относительно ДМП информационных потоков, циркулирующих в том же фрагменте ССОП, в динамическом режиме.

Из данных утверждений следует, что разрабатываемая модель должна работать в двух режимах — статическом и динамическом, реализуя решение задачи расчета вероятности вскрытия элементов СТС (рис. 2).

Порядок функционирования модели следующий (рис. 2):

Таблица

Параметры потока, характеризующие узел сети

№ п/п	Поле	Описание
1	REMOTE_ADDR	Целевой IP-адрес
2	HTTPVIA	Адрес следующего транзитного участка
3	HTTP_X_FORWARDED_FOR	Исходный IP-адрес
4	MAC_ADDR	Физический адрес
5	PROTOCOL_TYPE	Тип протокола
6	PORT_NUMBER	Исходный порт
7	OS_TYPE	Тип операционной системы

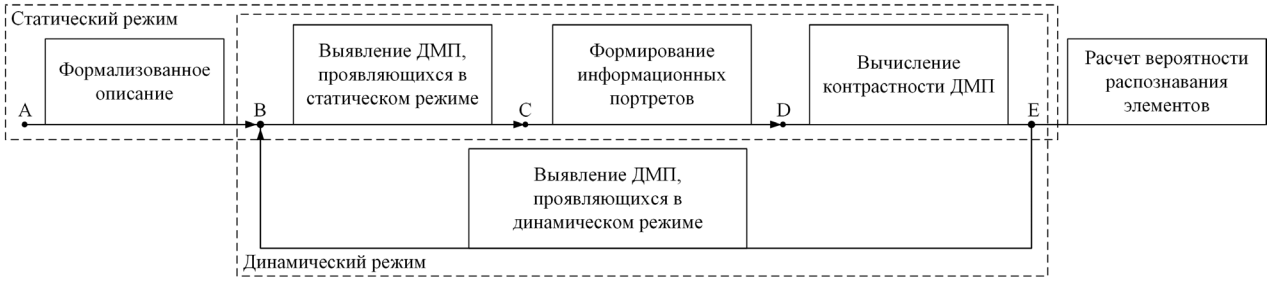

Рис. 2. Граф модели процесса распознавания элементов СТС

– в статическом режиме: подграф *ABCDE*, включающий первоначальное формализованное описание состояния системы и окружающей ее сети (ввод исходных данных), измерение ДМП элементов системы и элементов других систем связи, формирование информационных портретов (ИП), вычисление коэффициентов контраста ДМП элементов СТС относительно ДМП элементов других систем связи, расчет вероятности вскрытия каждого элемента СТС;

– в динамическом режиме: цикл *BCDEB*, включающий дополнительно контроль изменения алгоритмов функционирования, а также признакового пространства элементов корпоративной СТС и элементов ССОП в процессе функционирования системы, выявление ДМП передаваемых дейтаграмм, дополнение ИП.

Формирование ИП включает в себя:

1) определение района предполагаемого развертывания корпоративной СТС, состава задействованных технических средств ее элементов;

2) анализ элементов систем связи, функционирующих во фрагменте ССОП в предполагаемом районе развертывания СТС, измерение значений их параметров;

3) анализ элементов СТС, измерение значений их параметров, аналогичных проанализированным в п. 2;

4) нормирование значений параметров;

5) формирование векторов признаков для каждого элемента СТС;

6) формирование векторов признаков элементов систем связи фрагмента ССОП.

Значения векторов признаков всех элементов систем связи, функционирующих в одном фрагменте ССОП и доступных для средств ТКР, позволяют рассчитать контрастность каждого ДМП относительно «фона» и вычислить вероятность их распознавания.

Поскольку в исследуемом фрагменте ССОП при анализе ИП элементов систем связи нет ни априорных вероятностей появления образов классов, ни информации о распределении векторов наблюдений внутри классов, а также нет обучающих выборок, целесообразно для разбиения на классы (кластеры) использовать автоматическую классификацию (кластер-анализ) [8].

Исходная информация о классифицируемых объектах представлена в виде ИП, объединенных в матрицу признаков «объект-свойство»:

$$\mathbf{Z} = \begin{pmatrix} \vec{\mathbf{x}}^{\mathbf{1}^{\mathbf{T}}} \\ \dots \\ \vec{\mathbf{x}}^{\mathbf{N}^{\mathbf{T}}} \end{pmatrix} = \begin{pmatrix} \mathbf{x}_{\mathbf{1}}^{\mathbf{1}} & \dots & \mathbf{x}_{\mathbf{l}}^{\mathbf{1}} \\ \dots & \dots & \dots \\ \mathbf{x}_{\mathbf{1}}^{\mathbf{N}} & \dots & \mathbf{x}_{\mathbf{l}}^{\mathbf{N}} \end{pmatrix}, \qquad (1)$$

где x_j^n — значение j-го признака n-го объекта.

Задача классификации состоит в том, чтобы всю анализируемую совокупность $L \times N$ ИП элементов (1) разбить на сравнительно небольшое число Q однородных в определенном смысле классов (групп).

Классификация производится на основании расстояния $d(x_m, x_n)$, близкие относятся к одному классу, далекие к разным. В качестве расстояния выбрано взвешенное евклидово расстояние (2). Веса определены экспертным методом пропорционально степени важности компоненты x_i для отнесения объекта к тому или иному классу.

$$d_{WE}(\vec{x}^m, \vec{x}^n) =$$

$$= \sqrt{w_1(x_1^m - x_1^n)^2 + w_2(x_2^m - x_2^n)^2 \dots w_l(x_l^m - x_l^n)^2}, \qquad (2)$$

$$0 \le w_i \le 1, \sum w_i = 1.$$

Таким образом, распознавание объекта подразумевает успешное выполнение двух опера-

ций — обнаружение и классификацию. При этом между объектом и средствами разведки предварительно должен возникнуть контакт, а противнику заранее должны быть известны характеристики элементов СТС для их отнесения к определенному классу.

Источниками информации для ТКР являются:

1) данные, сведения и информация, обрабатываемые, в том числе передаваемые и хранимые, в инфокоммуникационных системах и сетях;

2) характеристики программных, аппаратных и программно-аппаратных комплексов;

3) характеристики пользователей инфокоммуникационных систем и сетей.

На рис. 3 представлена схема процесса взаимодействия ТКР с СТС, являющейся объектом разведки (ОР), в инфокоммуникационном пространстве. Здесь $\Theta(\vec{\mathbf{X}}_{\mathbf{E}}, \vec{\mathbf{Y}}_{\mathbf{E}}) = [x_1^m, x_2^m, ..., x_i^m, ..., x_k^m]$, $i = 1 \ldots N$, $m = 1 \ldots M$ — вектор параметров ДМП элемента СТС, действующий на входе датчика ТКР ($\vec{\mathbf{X}}_{\mathbf{E}}$ — полный вектор параметров ДМП собственно элемента СТС и элементов других сетей, находящихся в единой системе с ОР; $\vec{\mathbf{Y}}_{\mathbf{E}}$ — вектор оригинальных параметров элемента СТС, выделяющих его на фоне параметров других объектов); $\vec{\mathbf{F}}_{\mathbf{1}}(\mathbf{x}_{\mathbf{i}}^{\mathbf{1}})$, $i = 1 \ldots K$, $m = 1 \ldots M$ — вектор информационных параметров от объектов, локализованных устройством приема датчика ТКР, относительно определенной области пространства, пространственно-временным селектором $S_{x,m}$ [9].

Процесс распознавания протекает следующим образом: после приема множества сигналов средствами ТКР по совокупности параметров ДМП (координаты векторов $\vec{\mathbf{F}}_{\mathbf{1}}(\mathbf{x}_{\mathbf{i}}^{\mathbf{1}})$ на выходах селекторов $S_{x,m}$) проводится их сравнение с базой данных $\vec{\mathbf{X}}^{\mathbf{0}}(\mathbf{t},\mathbf{p})$ разведки (априорные пространственно-временные параметры возможных ДМП элементов СТС). На основе этого сравнения формируется правило:

$$\Delta X = \vec{\mathbf{F}}_{\mathbf{m}}(\mathbf{x}_{\mathbf{1}}^{\mathbf{m}}) S_{x,m} - \vec{\mathbf{X}}^{\mathbf{0}}(\mathbf{t},\mathbf{p}) \le \delta, \qquad (3)$$

где δ — установленный порог для принятия решения о присутствии в векторе $\vec{\mathbf{F}}_{\mathbf{1}}(\mathbf{x}_{\mathbf{i}}^{\mathbf{1}})$ признаков разведываемого вектора $\mathbf{Y(t, p)}$.

При выполнении условия (3) принимается решение об обнаружении и распознавании вектора $\mathbf{Y(t, p)}$ с вероятностью $P_{\text{расп эл}}$, и принятые данные в виде вектора $\mathbf{S}_{\mathbf{Y}}$ поступают в блок анализа параметров вектора $\mathbf{Y(t, p)}$ $\left(Y = \varphi(x)\right)$.

Таким образом, вероятность распознавания элемента СТС определяется по формуле

$$P_{\text{расп эл СТС}\,j}(t_{\text{ф}}) = \frac{1}{k} \sum\nolimits_{p=1}^{k} P_{\text{прхв}\,p}(t_{\text{ф}}) \cdot P_{\text{обн}\,p}(t_{\text{ф}}), \quad (4)$$

где $t_{\text{ф}}$ — время квазистационарного состояния системы СТС, k — количество ДМП j-го элемента СТС, $P_{\text{прхв}\,p}$ — вероятность перехвата p-го признака, $P_{\text{обн}\,p}$ — вероятность обнаружения p-го признака.

Вероятность перехвата — вероятность временного/территориального контакта средства ТКР с дейтаграммой, содержащей ДМП.

Вероятность обнаружения — вероятность принятия правильного решения о наличии признака путем выделения объекта на фоне других объектов.

Учитывая выражение (4), вероятность вскрытия СТС определяется выражением

$$P_{\text{вскр СТС}}(t_{\text{ф}}) = \frac{N_{\text{расп эл СТС}}}{N_{\text{эл СТС}}}, \qquad (5)$$

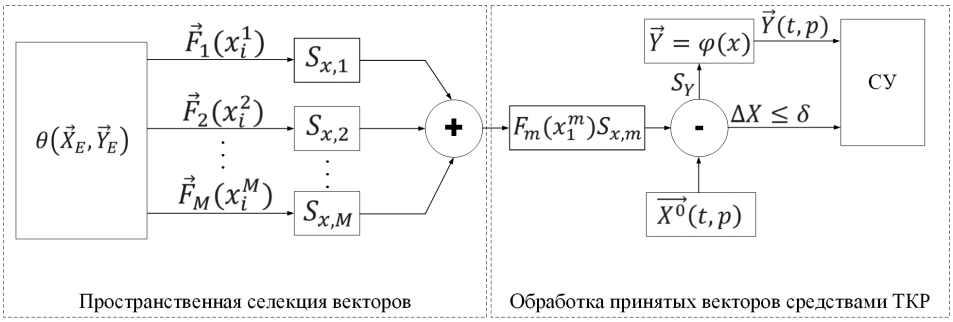

Рис. 3. Схема процесса взаимодействия ТКР с СТС, как объектом разведки

где $N_{\text{расп эл СТС}}$ — количество распознанных элементов СТС; $N_{\text{эл СТС}}$ — общее количество элементов СТС.

Исходя из вида разведки и ее возможностей, решаются следующие задачи:

– определяются ДМП, фиксируемые (регистрируемые) датчиками ТКР;

– оценивается возможность средств разведки по регистрации ДМП элементов СТС для конкретных условий функционирования;

– разрабатываются и реализуются практические меры по защите элементов системы;

– осуществляется контроль эффективности применяемых мер защиты СТС от ТКР.

Эталонные значения ДМП для обнаружения средствами ТКР могут быть получены путем перехвата и анализа сетевого трафика идентифицированных в том числе другими типами разведки узлов системы.

В модели введены следующие ограничения:

– район предполагаемого функционирования системы связи ограничен территорией Российской Федерации;

– структура ССОП задана и неизменна в течение модельного времени;

– узлы доступа (УД) характеризуются заданной производительностью;

– в рамках моделирования рассматривается множество ДМП СТС, доступных для обнаружения средствами ТКР;

– для передачи сообщений между элементами систем связи выбирается кратчайший маршрут по известному алгоритму;

– элементы характеризуются привязкой к УД ССОП, интенсивностью и направлением информационного обмена, а также набором параметров;

– модельное время не превышает длительности одного технологического этапа обмена информацией в системе связи.

Резюмируя отметим, что для решения задачи повышения разведзащищенности требуется выполнить следующие действия:

– заблаговременно в районе предполагаемого развертывания СТС выявить элементы функционирующих там систем связи;

– определить доступные для перехвата средствами ТКР ДМП выявленных элементов и измерить их значения;

– на основе полученных данных сформировать ИП каждого элемента систем связи;

– провести классификацию элементов со схожими ИП (объединить в группы);

– вычислить целевые показатели функционирования СТС (вероятность вскрытия).

Данные действия определяют порядок моделирования процесса распознавания элементов корпоративной СТС средствами ТКР (рис. 4).

Сначала задаются исходные данные. Далее моделируется функционирование ССОП, корпоративной СТС и других систем связи. На третьем этапе моделируется процесс функционирования ТКР. В заключение рассчитывается контрастность ДМП элементов СТС относительно элементов других систем связи и вероятность их распознавания на каждом шаге модельного времени. Используя данные значения вычисляется вероятность вскрытия системы.

В модели используются исходные данные, характеризующие сегмент ССОП: граф, задающий структуру (множество узлов, их производительность и линии связи между ними); исходные данные, характеризующие различные системы связи, функционирующие в рассматриваемом фрагменте ССОП: количество элементов данных систем, их привязку к узлам ССОП, нагрузку от каждого из них, закон ее распределения, а также матрицу информационных направлений; исходные данные, характеризующие корпоративную СТС: количество ее элементов, их привязку к узлам ССОП, нагрузку от каждого из них и закон

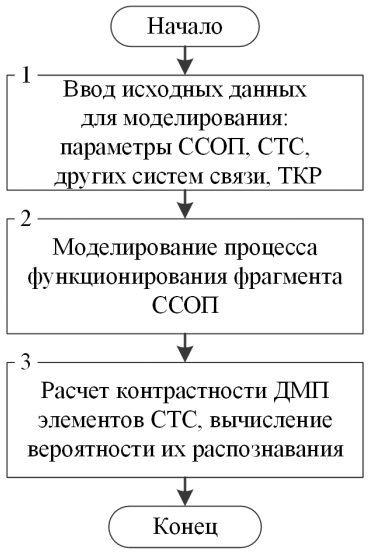

Рис. 4. Порядок моделирования

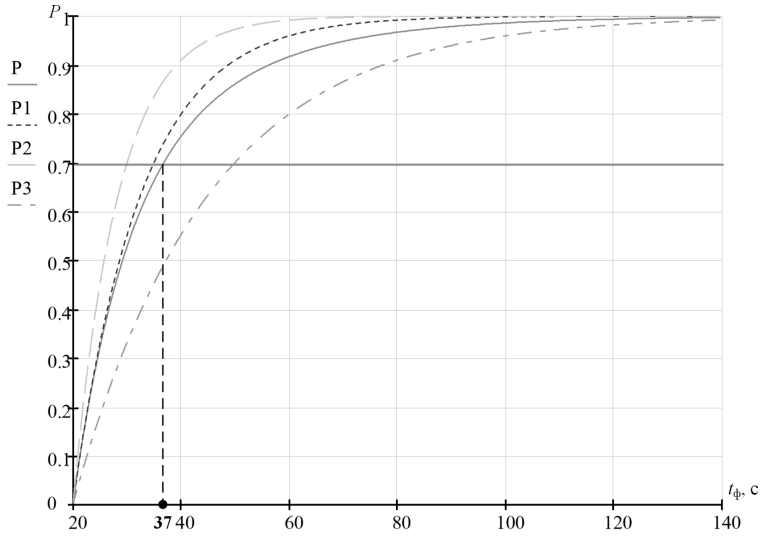

Рис. 5. Зависимость вероятностей распознавания трех элементов и вероятности вскрытия системы в целом от времени функционирования

ее распределения, матрицу информационных направлений; исходные данные, характеризующие противоборствующую сторону: количество датчиков ТКР, их привязку к узлам ССОП, интенсивность компьютерных атак со стороны каждого датчика и закон их распределения.

Выходными данными модели являются: вероятность распознавания каждого элемента корпоративной СТС средствами ТКР $P_{\text{расп}\,j}$, а также вероятность вскрытия всей системы связи $P_{\text{вскр СТС}}(t_ф)$, рассчитанные по выражениям (4) и (5) соответственно.

В результате расчетов с помощью модели получены значения целевых показателей функционирования корпоративной СТС в условиях действия ТКР. На рис. 5 представлены выходные результаты процесса моделирования. Выполнение расчетов произведено в последовательности, представленной на рис. 4. Исходные данные для модели собраны из дампа сетевого трафика фрагмента ССОП и введены в модель с помощью программного комплекса «Программное средство формирования данных модели распознавания элементов системы связи в инфокоммуникационном пространстве».

Анализ выходных данных показывает, что при времени квазистационарного состояния $t_ф \geq 37$ с система с вероятностью 0,7 будет вскрыта с помощью средств ТКР противоборствующей стороны. То есть, при расчетной длительности передачи информации, превышающей данное значение, необходимо принимать дополнительные меры по повышению разведзащищенности.

Моделирующие алгоритмы процессов распознавания элементов СТС средствами ТКР реализованы в программных средах Anylogic, python. Результаты оценки качества разработанной модели удовлетворяют общепринятым требованиям.

Выводы

В рамках моделирования предложено определение контрастности ДМП элемента инфокоммуникационной сети. Под контрастностью в данном контексте понимается относительное расстояние между значением ДМП элемента и средним значением данного ДМП среди всех элементов рассматриваемого фрагмента сети («фона»).

Представленная модель процесса обнаружения элементов корпоративной СТС средствами ТКР позволяет, в отличие от ранее известных, измерять значения ДМП элементов и рассчитывать их контрастность не только на основе появления эксплуатационных отказов, сбоев программного обеспечения, техногенных повреждений, факторов природного воздействия, деструктивных программных воздействий, но и учитывать значения параметров элементов сети, отображаемых в заголовке дейтаграммы.

Результатами моделирования являются сформированные векторы нормированных параметров элементов корпоративной СТС («информационные портреты»), коэффициенты контраста ДМП элементов, а также рассчитанные вероятности вскрытия элементов на каждом шаге модельного времени.

Литература

1. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С. 16–21.

2. Лепешкин О.М., Пермяков А.С., Шуравин А.С. Анализ возможностей нарушителя по контролю трафика в инфотелекоммуникационной сети. — СПб. Т. 1. 2020. С. 681–688.

3. Стародубцев Ю.И., Кузьмич А.А., Вершенник Е.В. и др. Способ моделирования виртуальной сети // Патент на изобретение RU № 2741262 C1, опубл. 22.01.2021. 23 с.

4. Коцыняк М.А., Лаута О.С., Нечепуренко А.П. Модель системы воздействия на информационно-телекоммуникационную систему специального назначения в условиях информационного противоборства // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2019. № 3–4 (129–130). С. 40–44.

5. Кучуров В.В., Максимов Р.В., Шерстобитов Р.С. Модель и методика маскирования адресации корреспондентов в киберпространстве // Вопросы кибербезопасности. 2020. № 6 (40). С. 2–13.

6. Меньшаков Ю.К. Основы защиты от технических разведок: учебное пособие. — М.: Изд. МГТУ им. Н.Э. Баумана. 2011. 478 с.

7. Панин С.Д. Теория принятия решений и распознавание образов. Курс лекций: учебное пособие. — М.: Изд. МГТУ им. Н.Э. Баумана. 2017. 239 с.

8. Бородачев С.М. Многомерные статистические методы: учебное пособие // Екатеринбург: УГТУ – УПИ. 2009. 84 с.

9. Burlov V.G., Lepeshkin O.M., Lepeshkin M.O., Gomazov F.A. The control model of safety management systems // В сборнике: IOP Conference Series: Materials Science and Engineering. 8th International Scientific Conference «TechSys 2019» — Engineering, Technologies and Systems. 2019. С. 012088.

References

1. Starodubtsev Yu.I., Zakalkin P.V., Ivanov S.A. Technosphere war as the main way of resolving conflicts in the context of globalization // Voyennaya mysl'. 2020. № 10. P. 16–21.

2. Lepeshkin O.M., Permyakov A.S., Shuravin A.S. Analysis of the intruder's capabilities to control traffic in the information telecommunications network. — SPb. Vol. 1. 2020. P. 681–688.

3. Starodubtsev Yu.I., Kuz'mich A.A., Vershennik Ye.V. and others. A method for modeling a virtual network // Patent for invention RU № 2741262 C1, publ. 22.01.2021. 23 p.

4. Kotsynyak M.A., Lauta O.S., Nechepurenko A.P. Model of the system of influence on the information and telecommunication system of special purpose in the conditions of information confrontation // Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2019. № 3–4 (129–130). P. 40–44.

5. Kuchurov V.V., Maksimov R.V., Sherstobitov R.S. Model and Methodology for Masking Correspondents Addressing in Cyberspace // Voprosy kiberbezopasnosti. 2020. № 6 (40). P. 2–13.

6. Menshakov Yu.K. Fundamentals of protection against technical intelligence: a tutorial. — M.: Izd. MGTU im. N.E. Baumana. 2011. 478 p.

7. Panin S.D. Decision theory and pattern recognition. Course of lectures: textbook. — M.: Izd. MGTU im. N.E. Baumana. 2017. 239 p.

8. Borodachev S.M. Multivariate statistical methods: a tutorial. — Yekaterinburg: UGTU – UPI. 2009. 84 p.

9. Burlov V.G., Lepeshkin O.M., Lepeshkin M.O., Gomazov F.A. The control model of safety management systems // In the collection: IOP Conference Series: Materials Science and Engineering. 8th International Scientific Conference «TechSys 2019» — Engineering, Technologies and Systems. 2019. P. 012088.