УДК 004.93.1

МЕТОДИКА ОБНАРУЖЕНИЯ И ИДЕНТИФИКАЦИИ КОМПЬЮТЕРНЫХ АТАК В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ МЕТОДА ИНДУКТИВНОГО ПРОГНОЗИРОВАНИЯ СОСТОЯНИЙ

Лаптев Владимир Николаевич
к.т.н., доцент
Кубанский государственный аграрный университет, Краснодар, Россия

Сидельников Олег Васильевич
Филиал Военной академии связи, Краснодар, Россия

В статье сформулированы показатели и критерии обнаружения компьютерных атак, разработаны модель и методика обнаружения компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний

Ключевые слова: МЕТОДИКА, МОДЕЛЬ, ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК, ИНДУКТИВНОЕ ПРОГНОЗИРОВАНИЕ СОСТОЯНИЙ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА

UDC 004.93.1

TECHNIQUE OF DETECTION AND IDENTIFICATION OF COMPUTER ATTACKS IN INFORMATION-TELECOMMUNICATION SYSTEMS ON THE BASIS OF THE METHOD OF INDUCTIVE FORECASTING OF CONDITIONS

Laptev Vladimir Nikolayevich
Cand.Tech.Sci., associate professor
Kuban State Agrarian University, Krasnodar, Russia

Sidelnikov Oleg Vasilevich
Filial of the Military Academy communication, Krasnodar, Russia

The article defines the parameters and criteria for detection of computer attacks; model and method of detection of computer attacks in the ITCS on the basis of the inductive pro-state forecasting are developed

Keywords: TECHNIQUE, MODEL, DETECTION OF COMPUTER ATTACKS, INDUCTIVE FORECASTING OF CONDITIONS, INFORMATION-TELECOMMUNICATION SYSTEM

Введение

Методика относится к области информационной безопасности информационно-телекоммуникационных систем (ИТКС) и может быть использована для обеспечения устойчивости функционирования ИТКС в условиях применения компьютерных атак [1-3].

Задача обеспечения защищенности ИТКС от компьютерных атак до настоящего времени решалась в большей части традиционными методами обеспечения безопасности информации (ОБИ). При этом было ярко выражено стремление, перекрыть все возможные каналы несанкционированного доступа (НСД) к данным, хранимым, обрабатываемым и передаваемым в сети. Основной недостаток такого подхода к ОБИ заключается в том, что злоумышленник знает результат своей атаки и в случае неудачи может выбрать такую стратегию атаки и (или) канал ее реализации, которая не будет обнаружена соответствующей системой ОБИ сети. Этот недостаток теории

становится все более существенным с увеличением масштабов и разнородности сети, спектра предоставляемых услуг, количества и качественного состава информационных ресурсов. Положение еще более усугубляется с ростом числа способов и изощренности компьютерных атак, которые уже направлены не только на данные, но и на многочисленные сетевые службы и могут осуществляться практически на всех уровнях эталонной модели взаимодействия открытых систем [4-7].

К настоящему времени в области обнаружения компьютерных атак преобладают методы на основе сигнатурного анализа признаков атак. Преимущество данных методов - высокая точность определения факта атаки, а очевидный недостаток - невозможность обнаружения атак, сигнатуры которых пока не определены. Поскольку время проведения сетевых атак зачастую ограничивается несколькими секундами, а время разработки сигнатур и пополнения базы данных сигнатур может занять от нескольких часов до нескольких дней, то отсюда можно сделать вывод о слабой пригодности этого метода в чистом виде для применения в системе выявления атак ИТКС [8].

Поведенческие методы, в отличие от сигнатурных, основаны на статистических методах анализа активности и базируются не на моделях компьютерных атак, а на моделях штатного процесса функционирования ИТКС. Принцип использования поведенческих методов заключается в обнаружении несоответствия между текущим режимом функционирования ИТКС и режимом штатной работы. Любое такое несоответствие в рамках поведенческого метода рассматривается как компьютерная атака. В отличие от сигнатурных, поведенческие методы позволяют выявлять не только известные, но и новые типы атак. Однако в большинстве случаев поведенческие методы характеризуются большим количеством ошибок, поскольку не всякое отклонение от штатного режима работы ИТКС является реальной компьютерной атакой [2, 4-7].

Поведенческие методы также реализуются при помощи нейросетей и экспертных систем. В последнем случае база правил экспертной системы описывает штатное поведение ИТКС. Процесс обучения с применением нейросетевых технологий начинается с предъявления системе набора обучающих примеров, состоящих из входных и выходных сигналов. Затем нейронная сеть автоматически подстраивает свои синоптические веса таким образом, что при последующем предъявлении входных сигналов на выходе получаются требуемые сигналы. Недостатком данного подхода являются трудности, возникающие при попытках семантической интерпретации механизмов работы нейронной сети. Кроме того, мало исследованным остается вопрос, каким образом представляются знания в нейронных сетях [6].

1. Постановка задачи

Обеспечение защищенности и устойчивости функционирования ИТКС в условиях массированного воздействия компьютерных атак осуществляется путем повышения вероятности обнаружения новых компьютерных атак и снижением времени распознавания признаков известных атак путем ограниченного перебора признаков атак в базе данных на основе применения метода индуктивного прогнозирования состояний [1].

При этом обнаружение компьютерных атак, ограниченный перебор признаков атак в базе данных и формирование базы знаний может осуществляться по известным [2, 4, 6, 7] методикам. ИТКС является объектом защиты от компьютерных атак. Анализ выполнения технологических циклов управления (ТЦУ) ИТКС и массированного воздействия компьютерных атак на узлы ИТКС показывает, что узлы будут выведены из строя и не смогут выполнять возложенные на себя функции по выполнению ТЦУ [2]. Необходимым элементом СЗИ от НСД в ИТКС при выполнении ТЦУ для обнаружения и противодействия массированного воздействия компьютерных атак должны быть средства обнаружения компьютерных атак. Вы-

явленные недостатки существующих методов обнаружения компьютерных атак показали, что ни один из методов не способен обнаруживать новые атаки в реальном масштабе времени. Временной параметр обнаружения компьютерных атак в ИТКС является одним из основных для оценки обстановки и принятия решения [2, 4].

Таким образом, используемые в настоящее время методы, алгоритмы и методики обнаружения компьютерных атак в ИТКС не разрешают противоречие между ограниченным временем на выполнение регламентов ТЦУ в условиях массированного воздействия компьютерных атак, с одной стороны, и временем, необходимым для обнаружения и противодействия компьютерных атак существующими методами, с другой. Попытка решить данное противоречие традиционными методами ведет к утрате устойчивости функционирования ИТКС.

Показатели и критерии. Под устойчивостью ИТКС понимается комплексное свойство ИТКС, характеризуемое живучестью, помехоустойчивостью и надежностью [8]. Где, под надежностью ИТКС понимается комплексное свойство ИТКС сохранять во времени в установленных пределах значения всех параметров, характеризующих способность ИТКС выполнять свои функции в заданных режимах и условиях эксплуатации. Под живучестью понимается свойство ИТКС, характеризуемое способностью выполнять установленный объем функций в условиях воздействий внешней среды и отказов компонентов системы в заданных пределах. Под помехоустойчивостью понимается свойство ИТКС, характеризуемое способностью выполнять свои функции в условиях воздействия помех [8]. Таким образом, устойчивость представляет собой слагаемое эффективности систем, которое характеризуется способностью противостоять внешним воздействиям. Под уровнем устойчивости функционирования ИТКС будем понимать качественный критерий, характеризующий интегральное свойство ИТКС выполнять целевую функцию при воздействии компьютерных сетевых атак.

Поэтому качественный критерий устойчивости должен согласовываться с критерием эффективности. Так как в качестве критерия эффективности как меры успешности выполнения заданной задачи принимается вероятность ее выполнения, то в качестве критерия устойчивости принята вероятность выполнения заданной задачи системой в условиях воздействия компьютерных атак.

Если обозначить $P_{выв}$ - вероятность вывода из строя (функциональное поражение [2]) ИТКС в результате воздействий компьютерных атак. Тогда от критерия вывода из строя $P_{выв}$ зависит способность ИТКС выполнять целевую функцию в условиях воздействия компьютерных атак. Поэтому величина $P_{уст} = 1 - P_{выв}$ может быть принята в качестве критерия устойчивости. Этот критерий определяет вероятность выполнения системой задачи в условиях воздействия компьютерных атак. Однако, вероятность вывода из строя зависит от системы защиты ИТКС от компьютерных атак, которую возможно выразить следующим образом,

$$P_{выв} = 1 - P_{ПР} P_{обн} \quad (1.1)$$

где $P_{ПР}$ - вероятность противодействия компьютерным атакам, а $P_{ОБН}$ - вероятность обнаружения компьютерных атак.

В связи с тем, что критерий противодействия зависит от обнаружения компьютерных атак, то примем допущение, что критерий вывода из строя ИТКС согласно (1.1) равен $P_{выв} = 1 - P_{обн}$, тогда $P_{уст} = 1 - (1 - P_{обн})$, следовательно, критерий устойчивости равен критерию обнаружения компьютерных атак.

$$P_{уст} = P_{обн}. \quad (1.2)$$

$$P_{обн} = \lim_{N \to \infty} \frac{N_a}{N}, \quad (1.3)$$

где N_a - количество обнаруженных атак; N - общее количество атак.

Теоретической основой методики являются теории множеств, рас-

познавания образов, аппарат математической логики, теория графов, системного анализа, вычислительной математики, методов инженерии знаний и построения экспертных систем, теория принятия решений и теории вероятностей, методы экспертных оценок и математического моделирования.

Исходные данные. Множество состояний ИТКС при реализации технологических циклов управления ИТКС:

$$S = \begin{Bmatrix} S_{00}, S_{01}, S_{02}, ...S_{0n} \\ S_{10}, S_{11}, S_{12}, ...S_{1n} \\ S_{k0}, S_{k1}, S_{k2}, ...S_{kn} \end{Bmatrix} \quad (1.4)$$

Множество компьютерных атак Ω, которое содержит матрицу классов атак $\Omega = \{A_1, A_2, A_3, ...A_m\}$, а каждый класс атак, например, $A_1 = \{A_{11}, A_{12}, A_{13}, ...A_{1n}\}$ включает в себя подмножество объектов атак данного класса, характеризуемых различными классификационными признаками $A_{11}, A_{12}, A_{13}, ...A_{1n}$ в зависимости от сложности, типа и формы компьютерной атаки.

$$\Omega = \begin{Bmatrix} A_1 = \{A_{11}, A_{12}, A_{13}, ...A_{1n}\} \\ A_2 = \{A_{21}, A_{22}, A_{23}, ...A_{2n}\} \\ A_3 = \{A_{31}, A_{32}, A_{33}, ...A_{3n}\} \\ A_m = \{A_{m1}, A_{m2}, A_{m3}, ...A_{mn}\} \end{Bmatrix}, \quad (1.5)$$

где $A_1, A_2, A_3, ...A_m$ – классы атак; A_{mn} – объект атаки с классификационным признаком mn.

Множество возможных действий по обнаружению компьютерных атак Ψ, которое включает в себя подмножество действий $\{И, К, П\}$. Где И – подмножество действий по идентификации компьютерной атаки, К – подмножество действий по классификации компьютерной атаки, т.е. отнесение идентифицированной атаки к определенному классу атак; П – подмножество действий, направленных на противодействие определенного класса атак. Индексы $\{1,2,...m\}$ относятся к определенным классам атак.

Например, $\{И_1\}$ - подмножество действий по идентификации класса атаки A_1; $\{И_2\}$ - подмножество действий по идентификации класса атаки A_2; $\{К_1\}$ - подмножество действий по классификации объекта атаки A_1; $\{П_1\}$ - подмножество действий, направленных на противодействие объекта атаки A_1.

$$\Psi = \begin{Bmatrix} a_1 = \{И_1, К_1, П_1\} \\ a_2 = \{И_2, К_2, П_2\} \\ a_3 = \{И_3, К_3, П_3\} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_m = \{И_m, К_m, П_m\} \end{Bmatrix}, \quad (1.6)$$

где $\{a_1, a_2, \ldots a_m\}$- подмножество действий по идентификации, классификации и противодействию компьютерным атакам.

Компьютерные атаки приводят к нарушению доступности информации пользователями ИТКС за счет нарушения ТЦУ, искажению информации, выдаче ложной информации и другие нарушения целостности и доступности информации в ИТКС.

Обеспечение устойчивого функционирования ИТКС в произвольный момент времени в условиях воздействия компьютерных атак достигается реализацией отображения:

$$P_{\text{ïîä}} : S \times \Omega \to S_{\text{ð}} = \left\{ S_p^{(i)} \right\}, \quad (1.7)$$

где S_p - множество разрешенных состояний ИТКС, соответствующих устойчивому функционированию при выполнении ТЦУ;

Ограничения. Функционал, определяющий обобщенный показатель эффективности обнаружения и противодействия компьютерным атакам и характеризующий устойчивость функционирования ИТКС, представим в следующем виде:

$$F = f\left[(\Omega, I), (S, t_{ТЦ}), (Y, M_{обн}, Z_{СОА})\right], \quad (1.8)$$

где Ω - множество компьютерных атак; I - множество распознаваемых образов компьютерных атак; S - множество состояний ИТКС при вы-

полнении ТЦУ; $t_{ТЦ}$ - время выполнения ТЦУ ИТКС; Y - параметр управления ИТКС; $M_{обн}$ - метод обнаружения компьютерных атак; $Z_{СОА}$ - средства обнаружения и противодействия компьютерным атакам.

При формировании набора параметров $M_{обн}^{ДОП}, Z_{СОА}^{Разраб}$ должны быть учтены ограничения j на те параметры, от которых зависят критерии эффективности обнаружения, идентификации и противодействия компьютерным атакам, в следующем виде:

$$j = \begin{Bmatrix} t_{нТЦ} \le t_{ТЦ} \le t_{кТЦ} \\ t_{обн} = t_{иден} + t_{кл} \end{Bmatrix}, \quad (1.9)$$

где $t_{нТЦ}, t_{кТЦ}$ - начальная и конечная стадия выполнения ТЦУ; $t_{обн}$ - время обнаружения компьютерной атаки; $t_{иден}$ - время идентификации компьютерной атаки; $t_{кл}$ - время классификации атаки.

Таким образом, подход к разработке методики сведен к выбору допустимых множеств параметров управления ИТКС, методов обнаружения компьютерных атак, направленных на идентификацию, классификацию и противодействие компьютерных атак для достижения максимума обобщенного показателя эффективности противодействия компьютерному нападению, обеспечивающего устойчивость функционирования ИТКС.

2. Модель обнаружения и идентификации компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний

Рассмотрим систему обнаружения атак с позиции теории динамических систем, которая изучает сложные структуры. По своей математической сущности ИТКС относится к динамическим системам и представляется в виде отношений множеств с определенными отношениями между элементами. Первое из этих множеств – совокупность входов (входных процессов, воздействий, возмущений – в нашем случае это компью-

терные атаки) второе – множество выходов (выходных процессов, откликов, реакций системы – действий направленных на обнаружение и противодействие компьютерным атакам).

Отношение, заданное на этой паре множеств, устанавливает связь между элементами.

Обозначим множество входов Ω - множество компьютерных атак (1.5), множество выходов - Ψ, множество действий, направленных на обнаружение и противодействие атакам (1.6), а множество состояний системы - S (1.4).

Тогда динамическую систему можно определить как некоторый абстрактный оператор, отображающий Ω в Ψ для фиксированных значений из S:

$$\Psi = F\left[S(\Omega)\right] \tag{2.1}$$

$$\Psi(t) = g\left[\Omega(t)\right] \tag{2.2}$$

$$\vec{\Psi}(t) = \vec{S}(t) \tag{2.3}$$

Компьютерная атака в нашем случае рассматривается как последовательность действий, приводящих систему из начального состояния в скомпрометированное (конечное) состояние.

Поведение системы характеризуется изменением во времени ее состояния $\vec{S}$, которое зависит от начального состояния $\vec{S}_0$ и входного воздействия $\vec{\Omega}$.

Если начальное состояние определить как состояние в некоторый момент времени $t_0 < t$, то можно записать:

$$\vec{S}(t) = F\left[\vec{S}(t_0), \vec{\Omega}(t), t\right], t_0 \le t \le t \tag{2.5}$$

при этом реакция на выходе системы будет:

$$\vec{\Psi}(t) = G\left[\vec{S}(t), \vec{\Omega}(t), t\right] \tag{2.6}$$

Соотношения (2.5) и (2.6) будут уравнением переменных состояний и уравнением наблюдения соответственно, а операторы F и G - операторами переходов и выходов системы.

Из непрерывности операторов F и G следует, что система может быть описана дифференциальным уравнением переменных состояния:

$$\frac{d\vec{\Omega}(t)}{dt} = \vec{\Omega}(t) = f\left[\vec{S}(t), \vec{\Omega}(t), t\right], \vec{S}(t_0) = \vec{S}_0, t \geq t_0 \qquad (2.7)$$

и уравнением наблюдения

$$\vec{\Psi}(t) = g\left[\vec{S}(t), \vec{\Omega}(t), t\right], \qquad (2.8)$$

где $f[.]$ и $g[.]$ - функции переходов и выходов.

Модель обнаружения компьютерных атак в условиях применения компьютерного нападения на ИТКС представлена на рисунке 2.1.

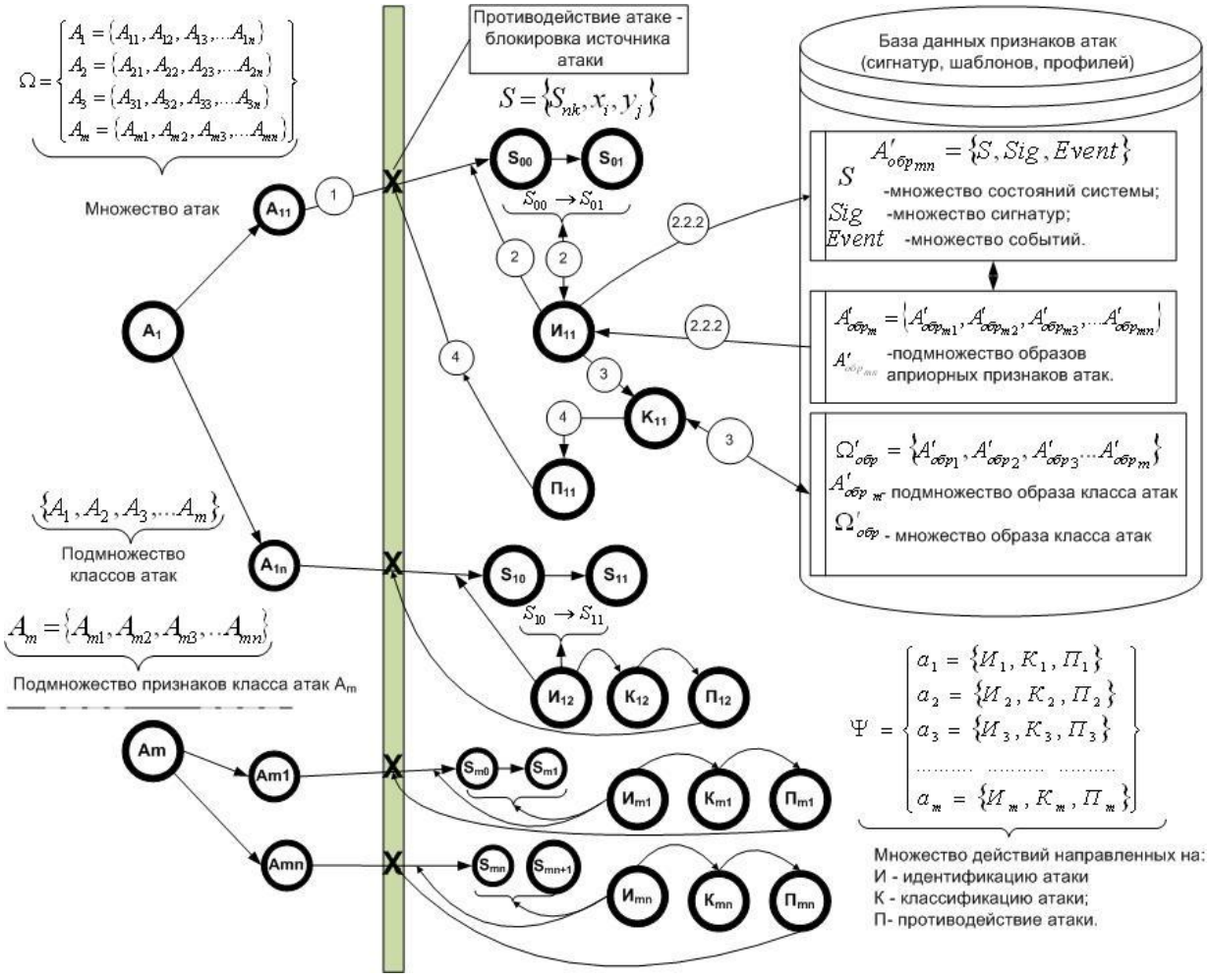

Рисунок 2.1 – Модель обнаружения и идентификации компьютерных атак на основе метода индуктивного прогнозирования состояний

На рисунке представлен граф состояний, состоящий из положений:

1. Проведение компьютерной атаки.

2. Идентификация компьютерной атаки, т.е. распознавание признаков атаки на основании изменения и перехода состояний системы $S = \{S_{nk}, x_i, y_j\}$, где S_{nk} - состояния системы, x_i - параметров и характеристик сетевого трафика, y_j - информация о работе аппаратного и программного обеспечения, пользователей ИТКС, а также средств защиты.

Множество возможных компьютерных атак Ω на ИТКС, хранящихся в базе данных атак (сигнатур, профилей и шаблонов) представим как распознаваемые образы атак для СОА в виде образов: $\Omega'_{обр} = \{A'_{обр1}, A'_{обр2}, A'_{обр3} ... A'_{обрm}\}$.

$$\Omega'_{обр} = \left\{ \begin{array}{l} A'_{обр1m} = \{A'_{обр11}, A'_{обр12}, A'_{обр13} ... A'_{обрm1}\} \\ A'_{обр2m} = \{A'_{обр21}, A'_{обр22}, A'_{обр23} ... A'_{обрm2}\} \\ A'_{обр3m} = \{A'_{обр31}, A'_{обр32}, A'_{обр33} ... A'_{обрm3}\} \\ ..... \\ A'_{обрmn} = \{A'_{обрm1}, A'_{обрm2}, A'_{обрm3} ... A'_{обрmn}\} \end{array} \right\} \quad (2.9)$$

где $\{A'_{обр1}, A'_{обр2}, A'_{обр3} ... A'_{обрm}\}$ - образы классов атак, а $A'_{обрmn}$ - классификационный признак образа атак A_{mn}.

Классификационный признак образа класса атаки характеризуется признаками для идентификации в виде

$A'_{обрm} = \{S, Sig, Event\}$:

где S - множество состояний системы $S = \{S_n, x_i, y_j\}$, характеризуемое подмножеством состояний и переходов системы, например переход из состояния S_0 в S_1: $S_0 \to S_1$; x_i - подмножество характеристик сетевого трафика; y_i - подмножество характеристик о работе аппаратного и программ-

ного обеспечения, пользователей ИТКС, а также средств защиты; *Sig* - подмножество сигнатур (признаков) или образов атак, хранимых в базе данных сигнатур и входящее в априорный алфавит классов компьютерных атак; *Event* - подмножество событий, например, событий НСД, обращений к системным файлам, события политики безопасности и т.д.

3. Классификация компьютерной атаки, т.е. отнесение ее к определенному классу атак.

4. Противодействие компьютерной атаке Ω, например, в виде блокировки источника атаки.

Таким образом, в рамках моделирования обнаружения и идентификации компьютерных атак в ИТКС:

- разработана модель на основе метода индуктивного прогнозирования состояний и получены зависимости состояний ИТКС, действий направленных на идентификацию, классификацию и противодействие компьютерным атакам;

- обоснован метод индуктивного прогнозирования состояний для обнаружения компьютерных атак в ИТКС.

3. Метод обнаружения и идентификации компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний

В [10] предложен подход к обнаружению компьютерных атак на основе метода индуктивного прогнозирования состояний. Идея метода распознавания заключается в следующем.

Рассмотрим множество объектов и обозначим его через *U*, полагая, что оно состоит из отдельных элементов, обозначаемых через u_j:$U=\{u_1,u_2,\ldots,u_m\}$. Множество всех признаков, используемых при описании этих объектов, обозначим через $S=\{s_1,s_2,\ldots,s_m\}$. Множество всех объектов, обладающих некоторым конкретным признаком s_j, обозначим через U_j,

называя его классом с признаком s_j, а его дополнение, т. е. множество всех объектов, не обладающих признаком s_j, – через $\overline{U}_j$.

Например, U может представлять адреса источника IP–дейтограмма, собираемые сетевыми датчиками для аудита, $s_1,s_2,\ldots,s_m$ – такие признаки, как октеты диапазона адресов: 192.168.1.16. U_3 – множество всех разрешенных адресов источника IP–дейтограмма, содержащиеся в третьем октете, $\overline{U}_3$ – множество не разрешенных адресов источника IP–дейтограмма, содержащиеся в третьем октете.

При исследовании реальных объектов мощность множества U, т. е. число элементов в нем, оказывается обычно очень большой, и, как правило, известна лишь относительно малая его часть. Предположим, что нам доступна вся информация об этом множестве и удалось описать каждый его элемент, перечислив признаки, которыми последний обладает, например, в виде $u_1-(s_1,s_2,s_4)$. Это означает, что объект представляет собой комбинацию признаков s_1, s_2 и s_4, т. е. обладает этими признаками и никакими другими. Доступную информацию можно представить иначе — строкой из нулей и единиц – булевым вектором. Символы строки соответствуют признакам s_1, s_2 ... и следует, что если объект обладает признаками: «1» – обладает, «0» – не обладает.

Рассмотрим объект с шестью признаками. Описание $u_1-(s_1,s_2,s_6)$ можно заменить на вектор: $[110001]$ (в данном случае число признаков ограничено шестью; при большем их числе вектор дополняется справа нулями).

Пользуясь такими средствами, можно представить множество U в целом. Для этого следует расположить друг под другом булевы векторы; представляющие последовательно объекты u_1,u_2 и т. д., получить булеву (из нулей и единиц) матрицу. Обозначим ее через R. Матрица содержит в удобной для обозрения форме информацию об отношении принадлежно-

сти признаков объектам: если объект U_j обладает признаком s_j, то на пересечении i-й строки и j-го столбца ставится «1», в противном случае – «0».

При больших ограничениях на используемые измерительные средства индивидуальность объектов может быть потеряна. Тогда отдельные строки матрицы R будут служить уже не моделями каких-то единичных объектов, а представлять их целыми группами, говоря о том, что в множестве U существуют объекты с заданными комбинациями признаков.

Строки матрицы являются R – группы объектов, неразличимых в данной системе признаков. Столбцы задают классы.

Множество всех таких комбинаций булевых векторов образуют так называемое булево пространство M. Множество U допустимых комбинаций является подмножеством из $U \subseteq M$. Назовем, это подмножество область существования объектов исследуемого класса, а его дополнение $\overline{U} = M \setminus U$ – область запрета, поскольку данное множество образуется запрещенными признаками. Всего их будет $41(2^6 = 64, 64 - 23 = 41)$.

$a \quad b \quad c \quad d \quad e \quad f$

$$R = \left|\begin{array}{cccccc|c} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 \\ 1 & 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 5 \\ 1 & 1 & 1 & 1 & 0 & 1 & 6 \\ 1 & 1 & 1 & 1 & 1 & 0 & 7 \\ 0 & 1 & 1 & 1 & 1 & 0 & 8 \\ 1 & 0 & 1 & 1 & 0 & 1 & 9 \\ 1 & 0 & 0 & 0 & 0 & 11 & 10 \\ 0 & 0 & 0 & 0 & 0 & 0 & 11 \\ 0 & 0 & 1 & 0 & 1 & 0 & 12 \\ 1 & 1 & 0 & 1 & 0 & 1 & 13 \\ 0 & 1 & 0 & 1 & 0 & 0 & 14 \\ 1 & 0 & 1 & 0 & 0 & 0 & 15 \\ 0 & 0 & 1 & 0 & 0 & 00 & 16 \\ 0 & 1 & 1 & 0 & 1 & 0 & 17 \\ 1 & 1 & 1 & 0 & 0 & 1 & 18 \\ 0 & 1 & 1 & 0 & 0 & 0 & 19 \\ 0 & 0 & 0 & 1 & 0 & 0 & 20 \\ 1 & 0 & 0 & 1 & 1 & 1 & 21 \\ 1 & 1 & 1 & 1 & 1 & 1 & 22 \\ 0 & 0 & 0 & 1 & 1 & 0 & 23 \end{array}\right| \quad (3.1)$$

Описания множеств U и $\overline{U}$ в целом эквивалентны (из одного можно получить другое), однако отдельные элементы этих множеств содержат информацию существенно различного типа — с точки зрения задач распознавания. Так, знание даже одного из элементов множества запрета $\overline{U}$, т. е. информация о том, что некоторый объект не существует, позволяет иногда решать задачу распознавания, в то время как аналогичные сведения о существовании некоторого объекта оказываются недостаточными для этого.

Запрет - это запрет на некоторые комбинации признаков: утверждается, что не существует объектов с такими комбинациями.

Под закономерностью понимается некоторые связи между признаками наблюдаемых явлений, причем достаточно сильные, чтобы их можно было обнаружить при наблюдении лишь отдельных, случайно выбранных объектов из исследуемого класса при условии, что выборка будет представительной: объекты выбираются независимо друг от друга и в достаточном количестве [11-12].

Чем больше запретных комбинаций, тем сильнее задающая запрет связь. Самая слабая связь задается каким либо одним элементом множества запрета $\overline{U}$ - когда именно он и запрещен. Обнаружить такую связь очень трудно. В общем случае связь охватывает несколько признаков, причем самая слабая — все признаки. Допустим, что связаны r признаков ($r \le n$) и эта связь представляется запретом некоторой комбинации их значений. Отобразим ее уже не булевым, а троичным вектором, компоненты которого принимают значения из трехэлементного множества $\{0,1,-\}$. При этом значением 0 или 1 будут обладать r компонент, соответствующих связываемым признакам, а остальные $n-r$ компонент получат значение $\{-\}$, являющееся символом неопределенности. Связь такого вида назовем импликативной связью ранга r. Элементарная связь оказывается, таким образом, частным случаем импликативной $\{-\}$ при $r = n$.

Анализируя множество U, легко убедиться в существовании импликативной связи, представляемой троичным вектором $\{1--01-\}$ и утверждающей, что не существует объектов, не обладающих определенными признаками.

Связь заданная вектором $\{1--01-\}$ или соответствующей ему элементарной конъюнкции $a\overline{d}e$ (логического произведения $a \wedge \overline{d} \wedge e$ трех сомножителей) означает, что не может быть так, чтобы некоторый объект обладал признаками a и e и не обладал признаком d. Это утверждение можно представить в форме импликации: «если объект обладает признаком a и не обладает признаком d, то он не обладает и признаком e» и выразим формулой:

$$a\overline{d} \to \overline{e} \qquad (3.2)$$

Очевидно, будет равносильно: $ae \to d$ и $\overline{d}e \to \overline{a}$.

В данном случае импликативная связь, заданная конъюнкцией $a\bar{d}e$, порождает восемь импликаций, включая и три приведенных выше: $a\bar{d}e \to 0$, $a \to d \vee \bar{e}$, $\bar{d} \to \bar{a} \vee \bar{e}$, $e \to \bar{a} \vee d$, $a\bar{d} \to e$, $ae \to d$, $\bar{d}e \to \bar{a}$, $1 \to \bar{a} \vee d \vee \bar{e}$.

Данный пример можно отобразить с помощью карт Карно, использующую симметричный код Грея, который каждому натуральному числу, начиная с нуля, ставит в соответствие свою кодовую комбинацию булев - вектор константу, число компонент в котором выбирается в зависимости от кодируемых чисел. При построении самого алгоритма распознавания не обязательно пользоваться картой Карно, тем более, что при больших признаков это практически невозможно. Альтернативой является алгебраический подход, сводящий распознавание к решению логических уравнений [12, 13].

Для этого достаточно подставить в исходную Дизъюнктивную нормальную форму (ДНФ) запрета, например

$$j = ac\bar{f} \vee b\bar{e}f \vee \bar{a}\bar{d}e \vee \bar{b}df \vee \bar{b}\bar{c}\bar{d} \qquad (3.3)$$

значения $a = 1$ и $f = 0$, преобразовав функцию j к частному виду, соответствующему именно этим значениям:

$$j(a = 1, f = 0) = 1 \cdot c\bar{f} \vee b\bar{e} \cdot 0 \vee 0 \cdot \bar{d}e \vee \bar{b}d \cdot 0 \vee \bar{b}\bar{c}\bar{d} = c \vee \bar{b}\bar{c}\bar{d} = c \vee \bar{b}\bar{d}$$

Таким образом, знание даже одного элемента множества запрета $\bar{U}$, т.е. информация о том, что некоторый объект не существует, позволяет иногда решить задачу распознавания, в то время, как аналогичные сведения о существовании некоторого объекта оказываются недостаточными для этого. Поэтому формулировку закономерностей, позволяющих решить задачи распознавания признаков компьютерных атак, будем связывать с запретами, т.е. запрет на некоторые комбинации признаков, что позволит

осуществлять не весь перебор возможных признаков атак в базе данных, а ограничиться сокращенным перебором.

При использовании метода индуктивного прогнозирования состояний компьютерная атака рассматривается как последовательность действий, приводящих систему из начального состояния в скомпрометированное (конечное) состояние. Таким образом, атака моделируется как множество состояний и переходов между ними. Состояние системы рассматривается как набор переменных, описывающих объекты, представленных в сигнатуре атаки. Начальное состояние ассоциируется с состоянием до выполнения атаки, а скомпрометированное состояние соответствует состоянию по окончании атаки. Переходы из состояния в состояние ассоциируются с новыми событиями в системе, влияющими на исполнение сценария атаки (например, запуск приложения, открытие TCP–соединения и т.д.). Типы допустимых событий (состояний системы) хранятся в базе данных. Между начальным и скомпрометированным состояниями существует множество переходов.

Такой способ позволяет:

- описать атаку более абстрактно, чем на уровне системных вызовов, и более точно, чем с использованием неформального текстового описания;

- выделить основные события в ходе выполнения атаки.

Таким образом, ключевыми факторами применимости метода индуктивного прогнозирования состояний являются следующие:

в связи с увеличением количества параметров (признаков) атаки, учитываемых в модели анализа состояний используется метод индуктивного вывода, основанный на распознавании признаков атак, связанных с запретами, т.е. запрет на некоторые комбинации признаков, что позволит осуществлять не весь перебор возможных признаков атак в базе данных, а ограничиться сокращенным перебором;

индукция подразумевает наличие достаточно представительной выборки обучающих примеров, которая обобщается посредством сгенерированных правил, позволяющая модифицировать базу знаний СОА ИТКС в автоматическом режиме и сформировывать новые правила и удалять старые;

скомпрометированное состояние должно быть распознано без использования внешних знаний о намерениях нарушителя (трудно обнаружить атаку маскарада с использованием учетной записи легитимного пользователя и корректного пароля).

4. Методика обнаружения и идентификации компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний

Последовательность выполнения методики обнаружения и идентификации компьютерных атак на основе метода индуктивного прогнозирования состояний представлена по этапам на рисунке 4.1.

Рисунок 4.1 – Этапы методики обнаружения и идентификации компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний

1 Этап - идентификация компьютерных атак.

1.1 Определение рабочего алфавита классов и рабочего словаря признаков компьютерных атак.

Классификация идентификационных характеристик сетевого трафика по уровням модели взаимодействия открытых систем, циркулирующего в ИТКС представлена в таблице 4.1 и информация о работе аппаратного и

программного обеспечения, пользователей ИТКС, а также средств защиты в таблице 4.2.

Таблица 4.1- Классификация идентификационных характеристик о сетевом трафике, циркулирующем в ИТКС

Группа характеристик протокола, уровень модели ВОС	Номер характеристики	Описание характеристики
Поля заголовков Ethernet-пакета	x_1	Тип протокола
Поля заголовков ARP, Канальный	x_2 - x_8	Длина MAC-адреса в байтах; длина адреса для используемого протокола; тип операции; MAC-адрес отправителя; IP-адрес отправителя; MAC-адрес получателя; IP-адрес получателя
Поля заголовков IP-пакета, Сетевой	x_9 - x_{21}	Версия протокола; количество 32 битных слов в заголовке пакета; желаемое качество обслуживания пакета; общая длина IP- пакета; идентификатор пакета; флаг, который должен всегда быть равен нулю; флаг фрагментированности пакета; флаг последнего в цепочке фрагментированных пакетов; позиция фрагмента внутри пакета; время в секундах, в течении которого пакет может находиться в сети; тип транспортного протокола, используемого при передаче; контрольная сумма; переменное число 32 битных слов
Поля заголовков ICMP-пакета, Сетевой Поля заголовков TCP, Транспортный	x_{22} - x_{25} x_{26} – x_{40}	Тип ICMP-сообщения; код функции соответствующего ICMP-сообщения; контрольная сумма; содержимое сообщения Номер TCP -узла отправителя; номер TCP - узла получателя; номер последовательности соответствующий данному сегменту; номер последовательности, который хочет получить узел следующим; длина TCP –сегмента; зарезервированное поле; признак того , что поле UrgentPointer значимо; признак того , что поле Acknowledgment-Number значимо; флаг PSH; флаг - признак обрыва соединения; флаг - признак синхронизации номеров последовательности; флаг - признак завершения соединения; размер окна; контрольная сумма; указатель на конец срочных данных в сегменте
Поля заголовков UDP, Транспортный	x_{41} - x_{44}	Номер UDP -порта отправителя и получателя; номер UDP -порта получателя; длина UDP-пакета; контрольная сумма
Поля заголовков HTTP, Прикладной	x_{47} - x_{51}	имя ресурса, к которому адресован HTTP; параметры заголовков HTTP; длина HTTP; тип метода, при помощи которого сформирован HTTP; имя ресурса, к которому адресован HTTP
Поля заголовков SMTP, Прикладной	x_{52} - x_{57}	электронный адрес отправителя и получателя сообщения; электронный адрес получателя сообщения; тема сообщения; информация о файловых вложениях; параметры заголовков SMTP-сообщения; информация о командах, передаваемых в рамках протокола SMTP
Поля заголовков FTP, Прикладной	x_{58} - x_{59}	адрес ресурса, к которому адресован FTP- запрос; информация о командах, передаваемых в рамках протокола FTP

Таблица 4.2 - Классификация информация о работе аппаратного и программного обеспечения, пользователей ИТКС, а также средств защиты

Группа характеристик информации	Номер характеристики	Описание характеристики

Информация об аппаратном обеспечении ИТКС	y_1	Вычислительная загрузка процессора
	y_2	Объем свободной оперативной памяти
Информация о работе общесистемного ПО	y_3	Информация о списке запущенных процессов
Информация о работе пользователей ИТКС	y_4	Время работы пользователя в системе
	y_5	Информация о приложениях, запущенных пользователями
Информация о работе средств защиты ИТКС	y_6	Количество заблокированных попыток доступа
	y_7	Информация о пакетах, зарегистрированных МЭ

1.2 Использования алгоритма распознавания компьютерных атак на основе метода индуктивного прогнозирования состояний.

1.2.1 Выбор критериев распознавания компьютерных атак.

1.2.2 Идентификация признаков компьютерных атак на основе метода индуктивного прогнозирования состояний.

1.2.2.1 Простые решения (стандартные задачи).

1.2.2.2 Решения прямыми логическими вычислениями.

1.2.2.2.1 Формирование классификационных признаков новых атак.

1.2.2.3 «Неразрешенные задачи» данной системой распознавания.

1.2.2.1.1 Формирование библиотеки «неразрешенных задач», подготовленной для решения более мощной системой.

2 Этап - классификация компьютерных атак.

3 Этап - противодействие компьютерным атакам.

Таким образом, в рамках разработки методики обнаружения компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний:

- определены этапы и последовательность действий для реализации методики обнаружения компьютерных атак и

- сформированы условия для разработки алгоритма обнаружения и идентификации компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний.

5. Алгоритм обнаружения и идентификации компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний

Шаг 1. Формирование пространства признаков.

На основе примера (2.8), допустим, предметами обнаружения и идентификации служат объекты некоторые класса, моделируемые в булевом пространстве признаков a, b, c, d, e, f. Предположим, что на этапе обучения наблюдению подверглось 64 конкретных объектов, в результате чего составлена таблица, в которой некоторые строки могут обладать одинаковыми значениями.

Таблица 5.1- Формирование пространства признаков

	a	*b*	*c*	*d*	*e*	*f*
Объект 1	1	1	0	1	0	0
Объект 2	0	1	1	1	1	1
…….						
Объект 64	0	0	1	0	0	0

Шаг 2. Построение модели исследуемого класса в алгебраической форме:

- в виде ДНФ запрета, если признаков минимально;
- в виде характеристической функции – булева функции запрета.

В рассматриваемом примере при построении модели класса видим пустыми интервалы третьего ранга и выдвигаем гипотезу о соответствующих импликативных закономерностях.

Предположим, что среди интервалов, ранги которых не превышают трех, пустыми оказались лишь те, которые представлены строками следующей троичной матрицы:

Эта матрица будет моделью исследуемого класса. Строки интерпретируются как импликативные закономерности: первая строка утвержда-

a b c d e f

$$T=\begin{bmatrix} 1 & - & 1 & - & - & 0 \\ - & 1 & - & - & 0 & 1 \\ 0 & - & - & 0 & 1 & - \\ - & 0 & - & 1 & - & 1 \\ - & 0 & 0 & 0 & - & - \end{bmatrix} \quad (5.1)$$

ет, что в данном классе не существует объектов, обладающих признаками a и c, но не обладающих в тоже признаком f. Представим данную модель в алгебраической форме – посредством ДНФ запрета.

$$j = ac\bar{f} \vee b\bar{e}f \vee \bar{a}\bar{d}e \vee \bar{b}df \vee \bar{b}c\bar{d} \quad (5.2)$$

Шаг 3. Выбор целевого признака их системы закономерностей и упрощение.

Пусть в данном примере роль целевого признака играет признак – b.

При $b=0$ становится излишней строка 2, так как задаваемая ею область запрета не содержит элементов с таким значением признака b и следовательно, не пересекается с интервалом возможного существования объекта, не обладающего признаком b. Удалив ее вместе со столбцом b, получим остаток

$$T=\begin{array}{c} \begin{matrix} a & c & d & e & f \end{matrix} \\ \begin{bmatrix} 1 & 1 & - & - & 0 \\ 0 & - & 0 & 1 & - \\ - & - & 1 & - & 1 \\ - & 0 & 0 & - & - \end{bmatrix} \end{array} \begin{matrix} 1 \\ 3 \\ 4 \\ 5 \end{matrix} \quad (5.3)$$

Если, $b=1$, следует анализировать остаток матрицы T.

$$\begin{array}{c} \begin{matrix} a & c & d & e & f \end{matrix} \\ \begin{bmatrix} 1 & 1 & - & - & 0 \\ - & - & - & 0 & 1 \\ 0 & - & 0 & 1 & 1 \end{bmatrix} \end{array} \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} \quad (5.4)$$

Представим в графической форме алгоритм в виде дерева (рис.5.2).

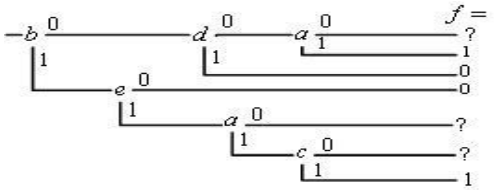

Рисунок 5.2 –Дерево идентификации признака f

Сформулируем алгоритм обнаружения и идентификации признаков:

1. Измерить признак b. Если $b=1$, перейти к п.2, если $b=0$, измерить признак d. Если $d=1$, приписать признаку f значение U и выйти на п.3. Если $d=0$, то измерить признак a. Если $a=1$, приписать признаку значение 1 и выйти на п.3. Если $a=0$, отказаться от обнаружения и идентификации, выйдя на п.3.

2. Измерить признак e. Если $e=0$, приписать признаку f значение 0 и выйти п.3. Если $e=1$ измерить признак a. Если $a=0$, отказаться от обнаружения и идентификации, выйдя на п.3. Если $a=1$, измерить признак c. Если $c=0$, отказаться от обнаружения и идентификации, выйдя на п.3. Если $c=1$, приписать признаку f значение 1 и отказаться от обнаружения и идентификации, и выйти на п.3.

3. Конец алгоритма.

При таком рассмотрении процесса обнаружении и идентификации признаков можно использовать из двух подходов, напоминающих интерпретацию и компиляцию в системном программировании.

6. Разработанная структура СОА ИТКС на основе метода индуктивного прогнозирования состояний

Разработанная структура СОА ИТКС включает в себя следующие компоненты (см. рисунок 6.1):

1. Модуль сбора данных (интеллектуальные датчики- датчик сенсор) для сбора исходных данных: сетевые пакеты, настройки, состояния системы, события, сообщения в системных журналах.

2. Модуль выявления атак на основе метода индуктивного прогнозирования состояний, предназначенного для идентификации компьютерных

атак. Основные его задачи:

формирование пространства признаков;

построение модели исследуемого класса в алгебраической форме и выбора целевого признака в виде характеристической функции – булева функции запрета или в виде дизъюнктивной нормальной форме запрета;

снижением размерности задачи за счет логических вычислений и декомпозиции ее на простые решения, решения задачи прямыми логическими вычислениями и упрощением до «неразрешенной» задачи.

3. Модуль хранения данных (сигнатур, шаблонов), предназначенный для классификации компьютерных атак.

4. База знаний, предназначенная для формирования классификационных признаков новых атак.

5. Модуль реагирования, предназначенный для противодействия компьютерным атакам.

6. Модуль управления, предназначенный для выдачи информации управления модулям СОА.

7. Библиотека «неразрешенных задач», предназначенная для отправки на анализ более мощной внешней системе обнаружения компьютерных атак.

Допускается, чтобы все эти компоненты функционировали на одном компьютере. Управление разработанной СОА ИТКС может осуществляться с технологического места администратором. В целом, разработанная структура СОА позволяет повысить эффективность обнаружения компьютерных атак в реальном масштабе времени, что важно для ИТКС за счет:

- ограниченного сокращенного перебора классификационных признаков известных атак в имеющейся базе данных признаков атак (сигнатур, шаблонов, профилей);

- формирования выборки обучающих примеров в базу знаний СОА, посредством сгенерированных правил;

- пополнения базы данных классификационными признаками новых атак.

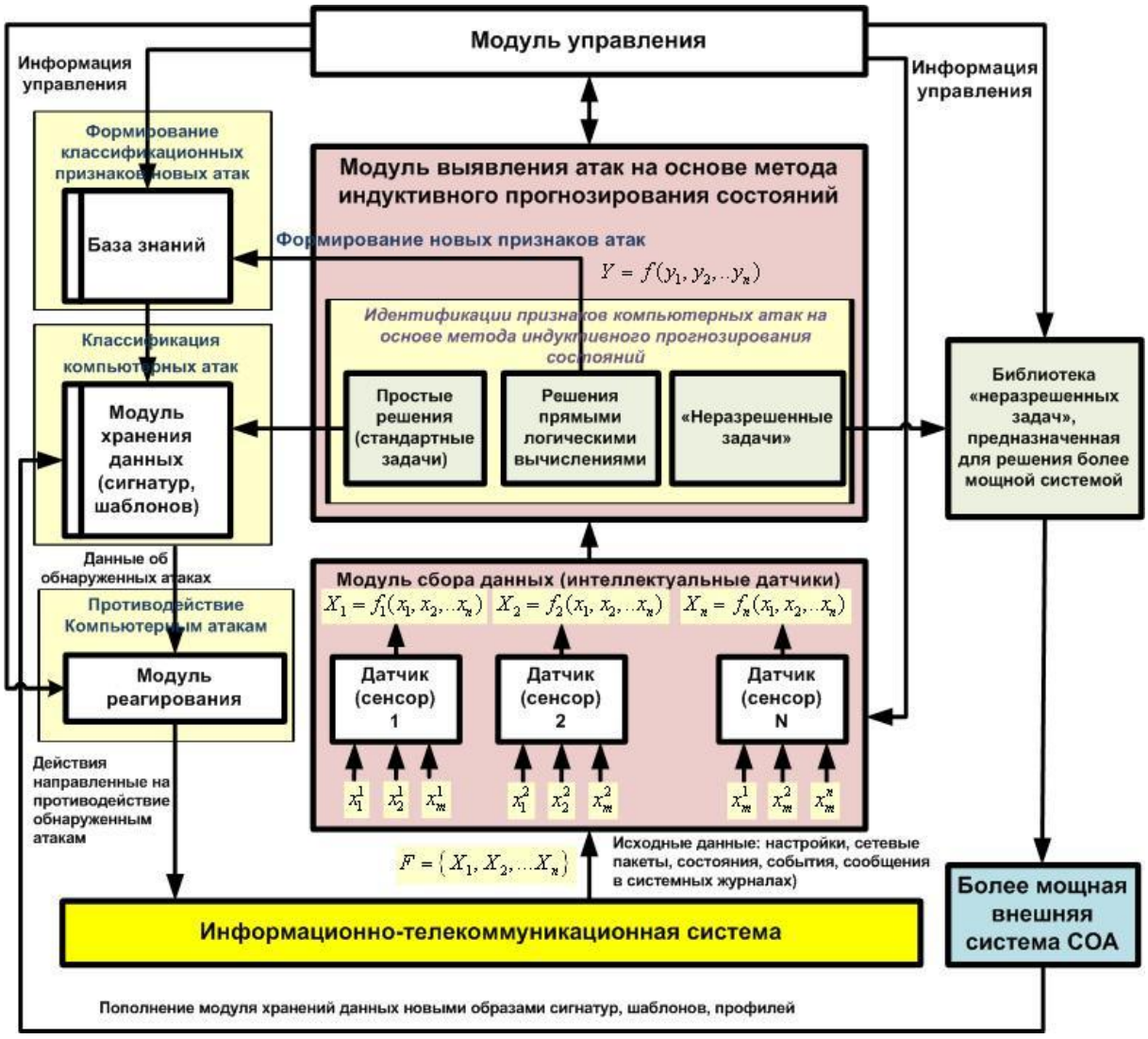

Рисунок 6.1 – Разработанная структура СОА ИТКС на основе метода индуктивного прогнозирования состояний

Для оценки устойчивости функционирования СОА ИТКС представлена как система массового обслуживания с отказами, которая состоит из 1 обслуживающего прибора, в который поступает пуассоновский поток компьютерных атак с интенсивностью λ для обнаружения и идентификации. Сравнение проводилось с общедоступной системой СОА Snort. Полученные результаты позволили сделать вывод о том, что применение метода индуктивного прогнозирования состояний для обнаружения и идентификации компьютерных атак в ИТКС в реальном масштабе времени

позволило повысить вероятность обнаружения компьютерных атак на 18%, тем самым повысить устойчивость функционирования ИТКС к компьютерным атакам.

Заключение

В статье сформулированы показатели и критерии обнаружения компьютерных атак, разработаны модель и методика обнаружения компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний.

В рамках моделирования обнаружения и идентификации компьютерных атак в ИТКС:

разработана модель обнаружения и идентификации компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний, отличающаяся от известных представлением ее в виде тройки множеств: «компьютерная атака», «состояние», «действия, направленные на обнаружение, классификацию и противодействие компьютерной атаки» и введением понятия «неопределенный» признак $\{-\}$, в результате чего комбинация признаков может быть представлена не булевым, а троичным вектором $\{0,1,-\}$.

обоснован метод индуктивного прогнозирования состояний для обнаружения компьютерных атак в ИТКС, отличительной чертой которого являются введением этапа выбора целевого признака исследуемого класса в алгебраической форме в виде характеристической функции – булева функции запрета или в виде ДНФ запрета и снижение размерности задачи за счет логических вычислений и декомпозиции ее на простые решения, решения задачи прямыми логическими вычислениями и упрощением до «неразрешенной» задачи.

В рамках разработки методики обнаружения компьютерных атак в ИТКС на основе метода индуктивного прогнозирования состояний:

- определены этапы и последовательность действий для реализации методики обнаружения компьютерных атак;

разработан алгоритм обнаружения и идентификации компьютерных атак, основанный на распознавании признаков атак, связанных с запретами на некоторые комбинации признаков, что позволяет осуществлять не весь перебор возможных классификационных признаков атак, а ограничиться сокращенным перебором.

Разработанные модель, методика обнаружения и идентификации компьютерных атак в ИТКС и разработанная структура СОА позволяют создать основу для синтеза надежных и высокопроизводительных адаптивных систем обнаружения компьютерных атак и позволяют сократить цикл разработки систем компьютерных атак нового поколения.

Направлениями дальнейших исследований являются разработка принципов снижения размерности решения задачи обнаружения и идентификации компьютерных атак за счет логических вычислений посредством алгебраических преобразовании; синтез специализированных программно-аппаратных устройств, способных к решению широкого класса задач обеспечения защищенности и устойчивости функционирования ИТКС в условиях применения компьютерного нападения.

Литература

1. Лаптев В.Н., Сидельников О.В., Шарай В.А. Применение метода индуктивного прогнозирования состояний для обнаружения компьютерных атак в информационно-телекоммуникационных системах. Научный журнал КубГАУ [Электронный ресурс]. – Краснодар: КубГАУ, 2011. – № 72(08). – 10 с. – Режим доступа: http://ej.kubagro.ru/2011/08/pdf/37.pdf.

2. Климов СМ., Методы и модели противодействия компьютерным атакам.- М: Люберцы.: КАТАЛИТ, 2008. – 316 с.

3. Приоритетные проблемы научных исследований в области обеспечения информационной безопасности Российской Федерации [Текст] : [Утверждены Исполняющим обязанности Секретаря Совета Безопасности Российской Федерации, председателя научного совета при Совете Безопасности Российской Федерации 7 марта 2008 г] – М. : 2007. – Режим доступа: http://www.scrf.gov.ru/documents/93.html.

4. Сердюк В.А. Новое в защите от взлома корпоративных систем. - Москва: Техносфера, 2007. – 306 с.
5. Корт С.С. Теоретические основы защиты информации: Учебное пособие. - М.: Гелиос АРВ, 2004. – 240 с.
6. Шангин В.Ф. Защита компьютерной информации. Эффективные методы и средства / Шангин В.Ф. - М.: ДМК Пресс, 2010. – 544 е.: ил.
7. Лукацкий А. В. Обнаружение атак. – 2-е изд. – СПб.: БХВ-Петербург, 2003. – 608 с.
8. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения. Введен в действие 01.01.1992.
9. Сидельников О.В., Коробка А.А. Анализ существующих методов обнаружения удаленных сетевых атак. // Перспективы развития средств и комплексов связи. Подготовка специалистов связи: Материалы межвузовской научной конференции. В 2 ч. Ч. 2 / Новочеркасское высшее военное командное училище связи. – Новочеркасск, 2009. – с. 56-61.
10. Закревский А.Д. Логика распознавания. Изд. 2-е, доп. – М.: Едиториал УРСС, 2003. – 200. – 144 с.
11. Закревский А.Д. Параллельные алгоритмы логического управления. Изд.2-е, стереотипное. – М.: Едиториал УРСС, 2003. – 200 с.
12. Закревский А.Д. Логические уравнения. Изд.2-е, стереотипное. – М.: Едиториал УРСС, 2003. – 96 с.