Содержание

Принятые сокращения

АПК	–	аппаратно-программный комплекс
АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
БД	–	база данных
КВИС	–	критически важная информационная система
ЛВС	–	локальная вычислительная сеть
МЭ	–	межсетевой экран
НСД	–	несанкционированный доступ
ОПО	–	общее программное обеспечение
ОС	–	операционная система
ПО	–	программное обеспечение
ППД	–	протокол передачи данных
СВТ	–	средства вычислительной техники
СЗИ	–	средства защиты информации
СПО	–	специальное программное обеспечение
СПКА	–	средства противодействия компьютерным атакам
СУБД	–	система управления базами данных
СЭП	–	сервер электронной почты
ТЦУ	–	технологический цикл управления
ЦКО	–	цифровое коммуникационное оборудование
ЭМ ВОС	–	эталонная модель взаимодействия открытых систем

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины	Определения
Критически важная информационная система (КВИС)	Информационно-телекоммуникационные средства, на которых осуществляются сбор, обработка и передача информации, выход параметров которых за допустимые пределы может привести к нарушению функционирования (функциональному поражению) КВИС.
Компьютерная атака	Целенаправленное программно-аппаратное воздействие на информационно-телекоммуникационные средства, приводящее к нарушению или снижению эффективности выполнения технологических циклов управления в КВИС.
Уязвимые места КВИС	Точки санкционированного и несанкционированного доступа, через которые могут быть реализованы компьютерные атаки.
Сценарий компьютерной атаки	Комплекс действий, проводимых с целью нарушения устойчивости функционирования КВИС.
Устойчивость функционирования КВИС	Способность КВИС обеспечивать установленные регламенты выполнения технологических циклов управления в условиях компьютерных атак.
Технология противодействия компьютерным атакам на КВИС	Совокупность взаимосвязанных процедур прогнозирования сценариев и классификации компьютерных атак нарушителя, анализа уязвимых мест и технологических циклов управления КВИС, применения методов и моделей противодействия атакам и оценки устойчивости функционирования КВИС в условиях компьютерных атак.
Показатель оценки противодействия компьютерным атакам	Характеристика одного из свойств средств предупреждения, анализа, обнаружения компьютерных атак и активного противодействия компьютерным атакам.
Шкала показателей оценки противодействия компьютерным атакам	Совокупность характеристик свойств средств реализации компьютерных атак, средств противодействия этим атакам и устойчивости функционирования КВИС.
Уровень устойчивости функционирования КВИС	Качественный критерий, характеризующий интегральное свойство КВИС выполнять ТЦУ при воздействии компьютерных атак.

1 Анализ существующих методов и моделей противодействия компьютерным атакам

В литературе по системам обнаружения и анализа компьютерных атак, приведенные методы не имеют достаточного математического описания. Как правило, они формализованы в виде способов и функций средств обнаружения компьютерных атак, используемых в инструментальных средствах средств предупреждения и обнаружения компьютерных атак (СПКА) [3, 6, 7, 25, 38, 40-43, 45-48, 58, 60]. Проблемные вопросы противодействия компьютерным атакам в современной литературе самостоятельного отражения не нашли, поэтому анализ рассматриваемых методов осуществлен для известных методов обнаружения и анализа атак.

Методы обнаружения и анализа компьютерных атак декомпозируются на:

– методы анализа сигнатур,

– методы обнаружения аномальных отклонений.

Классификация методов и моделей обнаружения и анализа компьютерных атак приведена на рисунке 1.

Методы анализа сигнатур предназначены для обнаружения известных атак и основаны на контроле программ и данных в критически важной информационной системе (КВИС) и эталонной сверке последовательности символов и событий в сети с базой данных сигнатур атак.

Исходными данными для применения методов служат сведения из системных журналов общего и специального программного обеспечения, баз данных и ключевые слова сетевого трафика КВИС.

Достоинством данных методов является незначительные требования к вычислительным ресурсам КВИС, сохранение высокой оперативности выполнения технологического цикла управления (ТЦУ) в КВИС и достоверности обнаружения и анализа атак.

Недостатком методов анализа сигнатур является невозможность обнаружения новых (модифицированных атак) без строгой формализации ключевых слов сетевого трафика и обновления базы данных сигнатур атак.

Методы обнаружения аномальных отклонений предназначены для обнаружения неизвестных атак. Принцип их действия состоит в том, что выявляется аномальное поведение КВИС отличное от типичного и на основании этого факта

принимается решение о возможном наличии атаки. Обнаружение аномальных отклонений в сети осуществляется по признакам компьютерных атак, таким как редкие типы стеков протоколов (интерфейсов) для запроса информации, длинные пакеты данных, пакеты с редкими распределениями символов, нестандартная форма запроса к массиву данных.

Рисунок 1 – Классификация методов и моделей обнаружения и анализа компьютерных атак

Для применения методов обнаружения аномальных отклонений и уменьшения числа ложных срабатываний необходимы четкие знания о регламентах обработки данных и требованиях к обеспечению безопасности информации (установленном порядке администрирования), обновлениях контролируемых программ, сведения о технологических шаблонах выполнения ТЦУ в КВИС.

Способы применения методов обнаружения аномальных отклонений различаются используемыми математическими моделями:

1) Статистическими моделями:
   – вероятностными моделями,
   – моделями кластерного анализа.
2) Моделями конечных автоматов.
3) Марковскими моделями.

4) Моделями на основе нейронных сетей.
5) Моделями на основе генной инженерии.

В методе обнаружения аномальных отклонений, в котором используются статистические модели, выявление аномальной активности осуществляется посредством сравнения текущей активности сетевого трафика КВИС с заданными требованиями к технологическому шаблону (профилю нормального поведения) выполнения ТЦУ КВИС.

В качестве основного показателя в вероятностных моделях обнаружения компьютерных атак используется:

- вероятность появления новой формы пакета передачи данных отличной от эталонной;
- математическое ожидание и дисперсия случайных величин, характеризующих изменение IP-адресов источника и потребителя информации, номеров портов АРМ источников и потребителей информации.

Статистические методы дают хорошие результаты на малом подмножестве компьютерных атак из всего множества возможных атак. Недостаток статистических моделей обнаружения аномальных отклонений состоит в том, что они не позволяют оценить объем передаваемых данных и не способны обнаружить вторжения атак с искаженными данными. Узким местом методов является возможность переполнения буфера пороговых проверок «спамом» ложных сообщений.

Для эффективного использования статистических моделей в методе обнаружения аномальных отклонений необходимы строго заданные решающие правила и проверка ключевых слов (порогов срабатывания) на различных уровнях протоколов передачи данных. В противном случае доля ложных срабатываний, по некоторым оценкам, составляет около 40 % от общего числа обнаруженных атак.

В основе моделей кластерного анализа лежит построение профиля нормальных активностей (например, кластера нормального трафика) и оценка отклонений от этого профиля посредством выбранных критериев, признаков (классификатора главных компонентов) компьютерных атак и вычислении расстояний между кластерами на множестве признаков атак. В моделях кластерного анализа используется двухэтапный алгоритм обнаружения компьютерных атак. На первом этапе осуществляется сбор информации для формирования множества данных кластеров аномального поведения КВИС на низших уровнях протоколов передачи данных. На втором этапе выполняется

сравнительный анализ полученных кластеров аномального поведения КВИС с кластерами описания штатного поведения системы.

Вероятность распознавания атак моделями кластерного анализа составляет в среднем 0,9 при обнаружении вторжений только по заголовкам пакетов передачи данных без семантического анализа информационной составляющей пакетов. Для получения достоверных данных с использованием моделей кластерного анализа необходим анализ порядка идентификации и аутентификации, регистрации абонентов, системных прерываний, доступа к вычислительным ресурсам в нескольких системных журналах КВИС: аудита, регистрации, ресурсов, что приводит к задержке времени на принятие решений. Такая задержка часто делает невозможным применение моделей кластерного анализа в системах квазиреального масштаба времени.

Обнаружение атак с использованием модели конечных автоматов основано на моделировании конечными автоматами процессов информационного взаимодействия абонентов КВИС по протоколам передачи данных. Конечный автомат описывается множествами входных данных, выходных данных и внутренних состояний. Атаки фиксируются по «аномальным» переходам КВИС из состояния в состояние. Предполагается, что в КВИС «штатные» переходы системы из состояния в состояние определены, а неизвестные состояния и переходы в эти состояния регистрируются как аномальные. Достоинством этой модели является упрощенный подбор классификационных признаков для КВИС и рассмотрение малого числа переходов из состояния в состояние. Модель позволяет обнаруживать атаки в потоке обработки данных сетевыми протоколами в режиме близком к реальному масштабу времени. К недостаткам модели следует отнести необходимость разработки большого числа сложных экспертных правил для сравнительного анализа требуемых и аномальных состояний и переходов системы. Экспертные правила оценки состояний КВИС взаимоувязаны с характеристиками сетевых протоколов передачи данных.

Методы обнаружения аномальных отклонений на основе марковских моделей основаны на формировании марковской цепи нормально функционирующей системы и функции распределения вероятностей перехода из одного состояния в другое. Эти сведения используются как обучающие данные. Обнаружение аномалий осуществляется посредством сравнения марковских цепей и соответствующих функций распределения вероятностей аномального и нормального функционирования КВИС по значениям порога вероятностей наступления событий. На практике эта модель наиболее эффективна для обнаружения компьютерных атак, основанных на системных

вызовах операционной системы, и требует дополнительных метрик условной энтропии для использования в системах квазиреального масштаба времени.

Методы обнаружения компьютерных атак на основе нейронных сетей применяют для предварительной классификации аномалий в КВИС. Они базируются на идентификации нормального поведения системы по функции распределения получения пакетов данных (выполнения заданных команд оператора), обучении нейронной сети и сравнительного анализа событий по обучающей выборке. Аномальное отклонение в КВИС обнаруживается тогда, когда степень доверия нейросети своему решению лежит ниже заданного порога. Предполагается, что применению модели нейронных сетей для реализации механизмов защиты информации КВИС от компьютерных атак предшествует обучение этих сетей заданным алгоритмам нормального функционирования. Недостатками методов обнаружения компьютерных атак с использованием нейронной сети являются сложный математический аппарат, который недостаточно эффективно работает в системах квазиреального масштаба времени, и сложность обучения сети для выявления неизвестных атак.

Модели обнаружения компьютерных атак на основе генной инженерии опираются на применение в сфере информационных технологий достижений генетики и моделей иммунной системы человека. Подход этой модели базируется на моделировании элементов иммунной системы человека в средствах обнаружения аномалий путем представления данных о технологических процессах в КВИС цепочкой (вектором) признаков и затем вычисления меры сходства между обучающей цепочкой признаков, характеризующих нормальное «поведение» КВИС и тестовой цепочкой, характеризующей аномальное функционирование. Если согласование между данными обучающей и тестовой цепочек не найдено, то процесс интерпретируется как аномальный. Одна из основных трудностей применения этой модели состоит в выборе порога согласования данных, формирования необходимого объема данных обучающей и тестовой выборки и чувствительности к ложным срабатываниям. Модель на основе генной инженерии (природной иммунной системы), применяется для обнаружения аномальных соединений по протоколу TCP/IP по данным об IP-адресах: источника информации, потребителя информации и коммуникационных средств, с помощью которой соединяются абоненты в сети.

Недостаток этих моделей заключается в том, что требуется сложная процедура настройки обучающей и тестовой выборок или данных о поведении индивидуума в КВИС с привлечением высококвалифицированного оператора.

Таким образом, достоинством методов обнаружения аномальных отклонений является возможность анализа динамических процессов функционирования КВИС и выявления в них новых типов компьютерных атак. Методы дают возможность априорного распознавания аномалий путем систематического сканирования уязвимых мест.

К недостаткам этих методов можно отнести необходимость увеличения нагрузки на трафик в сети, сложность реализации и более низкая достоверность обнаружения компьютерных атак в сравнении с сигнатурным анализом.

Ограничением методов обнаружения и анализа компьютерных атак является необходимость детальной информации о применении протоколов (стеков протоколов) передачи данных в КВИС на всех уровнях эталонной модели взаимодействия открытых систем (ЭМ ВОС).

Сравнительный анализ существующих методов обнаружения компьютерных атак по анализу сигнатур и аномальных отклонений в КВИС показал, что наиболее универсальным подходом к выявлению известных и неизвестных атак является метод обнаружения аномалий. Для повышения устойчивости функционирования КВИС необходим комбинированный метод противодействия компьютерным атакам, который гибко использует элементы сигнатурного анализа, выявления аномалий и функционального анализа динамически выполняемых функций КВИС.

2 СТРУКТУРА МЕТОДОВ И МОДЕЛЕЙ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ

Для эффективного решения задач противодействия компьютерным атакам на КВИС разработана структура методов и моделей противодействия компьютерным атакам, дополняющих существующие разработки (рисунок 2).

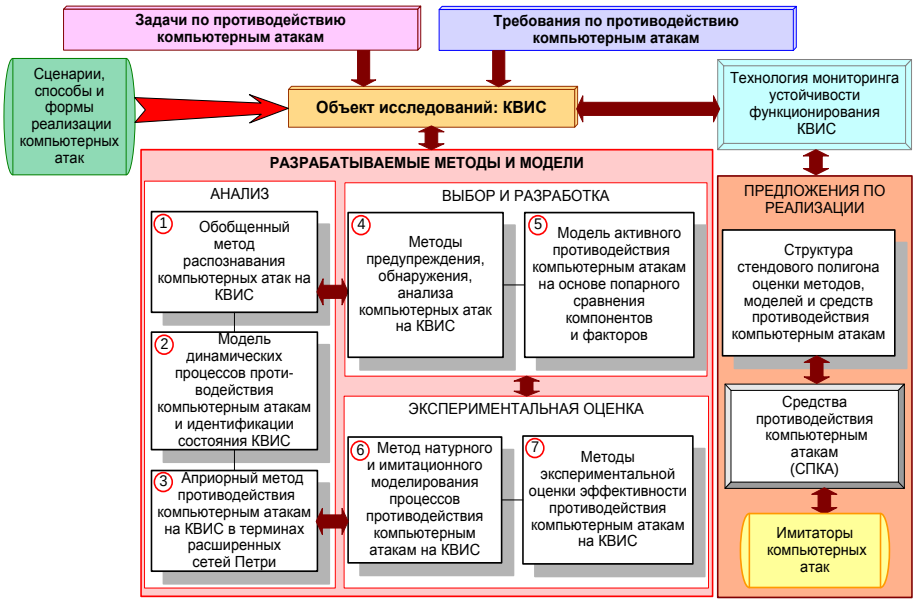

Рисунок 2 – Структура методов и моделей противодействия компьютерным атакам

Анализ рисунка 2 показывает, что объектом исследований при разработке методов и моделей противодействия компьютерным атакам являются критически важные информационные системы, выполняющие технологические циклы управления за ограниченное время и вероятность устойчивости функционирования которых, в условиях воздействия атак, должна быть не ниже заданной.

Представленные на рисунке 2 методы и модели должны позволять проведение:

– анализа сценариев, способов реализации и распознавание образов компьютерных атак потенциального нарушителя;
– идентификации состояния КВИС;
– априорного описания процессов противодействия атакам на КВИС в

терминах расширенных сетей Петри;

- предупреждения, обнаружения и анализа компьютерных атак на основе математически формализованных и согласованных логических правил;
- активного противодействия источникам компьютерных атак на основе метода анализа иерархий;
- экспериментальной оценки эффективности применения средств противодействия компьютерным атакам;
- обоснования стендового полигона для оценки методов, моделей и средств противодействия компьютерным атакам;
- обоснования требований и предложений по разработке средств противодействия компьютерным атакам.

Вопросы экспериментальной оценки эффективности применения средств противодействия компьютерным атакам на стендовом полигоне рассмотрены в электронном учебном пособии «Экспериментальная оценка противодействия компьютерным атакам на стендовом полигоне».

3 Подход к разработке методов и моделей противодействия компьютерным атакам

Целью разработки методических основ противодействия компьютерным атакам является обеспечение устойчивости функционирования КВИС в динамике ее применения и в условиях массированного воздействия компьютерных атак. Такая цель определяет подход к разработке методов и моделей противодействия компьютерным атакам, при котором необходимо взаимосвязано обеспечить защищенность и устойчивость функционирования КВИС.

Защищенность КВИС определяется применением традиционных и необходимых организационно-технических мероприятий, методов и средств защиты информации (СЗИ) от несанкционированного доступа (НСД), антивирусной защиты и выявления не декларированных возможностей в соответствии с требуемым классом защищенности автоматизированных систем и средств вычислительной техники [15-17]. Совершенствование сценариев и способов компьютерных атак нарушителя на КВИС и сами СЗИ с целью вывода их из строя приводит к необходимости наряду с традиционными методами и средствами защиты информации разрабатывать дополнительные методы и модели противодействия компьютерным атакам. Для обеспечения устойчивости функционирования КВИС в структуру СЗИ необходимо внедрить программные и программно-аппаратные датчики для извещения средств противодействия компьютерным атакам о состояниях информационной безопасности и устойчивой работе КВИС и ее СЗИ.

На рисунке 3 представлена обобщенная схема подхода к разработке дополнительных методов и моделей противодействия компьютерным атакам, которая отражает логику противодействия компьютерным атакам, а также комплекс методов, моделей, алгоритмов и средств, необходимых для обеспечения устойчивости функционирования КВИС в условиях воздействия компьютерных атак.

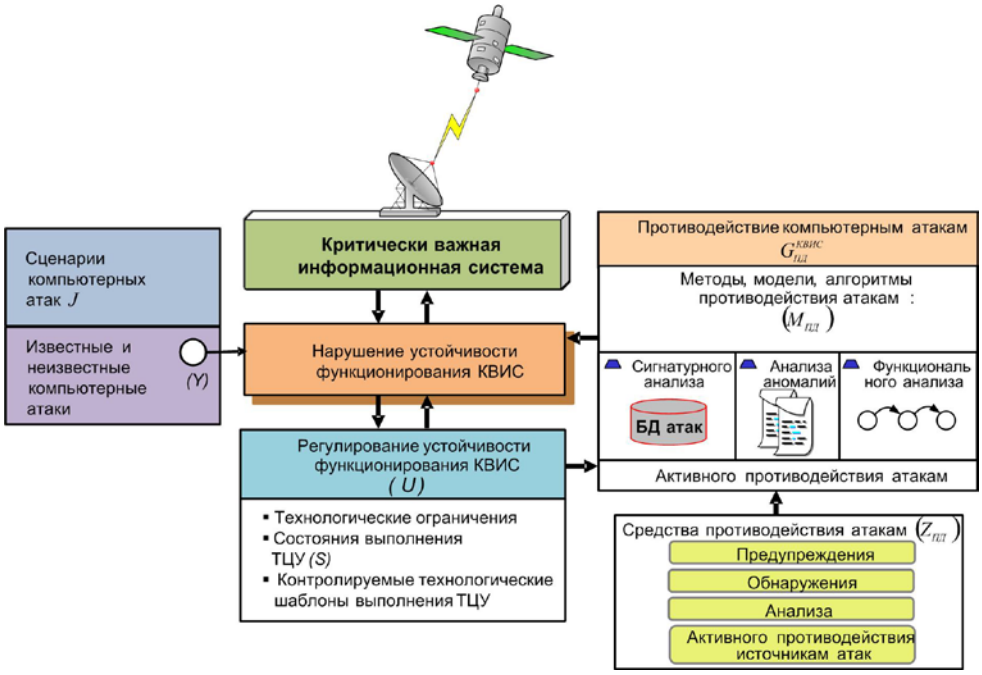

Рисунок 3 – Обобщенная схема подхода к разработке методов и моделей противодействия компьютерным атакам

Математическая формализация подхода к разработке методов и моделей противодействия компьютерным атакам на основе распознавания образов атак и идентификации состояния КВИС в виде теоретико-множественного представления осуществляется следующим образом.

Дано:

Множество состояний выполнения ТЦУ при реализации технологических операций сбора, обработки, передачи информации и выдачи управляющих воздействий на заданном интервале времени:

$$S = \{S_0, S_1, S_2, ..., S_N\}$$

Условия воздействия компьютерных атак, приводящие к нарушению ТЦУ, определяются множеством состояний реализации компьютерных атак:

$$Y = \{Y_0, Y_1, Y_2, ..., Y_K\}$$

Предположим, что компьютерные атаки приводят к искажению информации, выдаче ложной информации, к несвоевременной обработке данных и выдаче

информации абонентам в критические интервалы времени ТЦУ, а также к другим нарушениям целостности и доступности информации в КВИС.

Тогда обеспечение устойчивого функционирования КВИС в произвольный момент времени в условиях воздействия компьютерных атак достигается реализацией отображения:

$$G_{ПД}^{КВИС} : S \times Y \to S_p = \{S_p^{(i)}\}, \quad (1)$$

где S_p – множество разрешенных состояний КВИС, соответствующих устойчивому функционированию при выполнении ТЦУ.

Такая реализация обеспечивается организацией взаимоувязанных процессов регулирования параметров КВИС U, методов и моделей противодействия компьютерным атакам $M_{ПД}$, комплекса средств предупреждения, обнаружения, анализа компьютерных атак, активного противодействия атакам $Z_{ПД}$.

Функционал, определяющий обобщенный показатель эффективности противодействия компьютерным атакам и характеризующий устойчивость функционирования КВИС представим следующим образом:

$$P_{УФ}^{КВИС} = F\left[(J,Y),(S,T_{ТЦУ},\xi_{уяз}),(U,M_{ПД},Z_{ПД})\right], \quad (2)$$

где множества параметров нарушителя:

J – сценариев компьютерных атак;

Y – распознаваемых образов компьютерных атак;

множество параметров КВИС:

S – идентификации состояний КВИС при выполнении ТЦУ в процессе сбора, обработки и передачи информации;

$T_{ТЦУ}$ – периода времени выполнения ТЦУ;

$\xi_{уяз}$ – уязвимостей программного и информационного обеспечения КВИС;

множества параметров противодействия компьютерным атакам:

U – параметров регулирования КВИС;

$M_{ПД}$ – методов и моделей противодействия компьютерным атакам;

$Z_{ПД}$ – средств предупреждения, обнаружения, анализа компьютерных атак и активного противодействия атакам.

Исходя из этого, для обеспечения устойчивости функционирования КВИС в условиях воздействия компьютерных атак требуется найти:

$$P_{УФ}^{*КВИС} = \underset{U^{ДОП}\in U,\, M_{ПД}^{ДОП}\in M_{ПД}, Z_{ПД}^{ДОП}\in Z_{ПД}}{Arg\max} P_{УФ}^{КВИС}\left[\left(U^{ДОП}, M_{ПД}^{ДОП}, Z_{ПД}^{ДОП}\right)\right] \Big| \varphi, \qquad (3)$$

где $U^{ДОП}$ – допустимые параметры регулирования КВИС;

$M_{ПД}^{ДОП}$ – допустимые для возможного применения методы и модели противодействия компьютерным атакам на основе распознавания образов атак и идентификации состояния критически важных информационных систем;

$Z_{ПД}^{ДОП}$ – допустимые для возможного применения средства предупреждения, обнаружения, анализа компьютерных атак и активного противодействия атакам.

Другими словами, необходимо на множествах допустимых параметров регулирования КВИС; методов и моделей противодействия компьютерным атакам, а также средств предупреждения, обнаружения, анализа компьютерных атак и активного противодействия атакам осуществить целенаправленный выбор таких элементов, декартово произведение, которых обеспечивает максимум функционала $P_{УФ}^{КВИС}$.

При формировании набора параметров $U^{ДОП}, M_{ПД}^{ДОП}, Z_{ПД}^{ДОП}$ должны быть учтены ограничения на те параметры, от которых зависит критерий эффективности противодействия компьютерным атакам, в следующем виде:

$$\varphi = \begin{cases} \sum_{j=1}^{m} \xi_{уязj} \le \left| \sum_{j=1}^{m} \xi_{уязj}^{УСТ} \right|, \\ T_{Н} \le T_{ТЦУ} \le T_{К}, \\ \Delta T_{\min} = \Delta T_{д}, \\ C_{ПД} \le C_{ЗД}, \\ Z_{ПД}^{ДОП}\left(t_{ПД}, Q\right) = 1 \end{cases} \qquad (4)$$

где $\xi_{уязj}$ – потенциальные уязвимости КВИС;

$\xi_{уязj}^{УСТ}$ – уязвимости, установленные в ходе системного анализа и мониторинга устойчивости функционирования КВИС;

$T_{ТЦУ}$ – период времени выполнения ТЦУ;

$T_Н, T_К$ – начальная и конечная стадии выполнения ТЦУ;

$\Delta T_д$ – период времени действия атак;

$\Delta T_{\min}$ – минимальный период времени действия атак;

$C_{ПД}$ – реальная стоимость средств противодействия атакам;

$C_{ЗД}$ – заданная стоимость средств противодействия атакам;

$t_{ПД}$ – время противодействия атакам;

Q – датчики обнаружения атак.

При этом множества допустимых параметров противодействия компьютерным атакам $U^{ДОП}, M_{ПД}^{ДОП}, Z_{ПД}^{ДОП}$ формируются как подмножества соответствующих множеств возможных вариантов регулирования параметров КВИС U, применения методов и моделей противодействия атакам $M_{ПД}$ и средств предупреждения, обнаружения, анализа атак и активного противодействия атакам $Z_{ПД}$.

На момент времени начала противодействия атакам параметры нарушителя и КВИС принимаются в качестве постоянных величин, а изменяются лишь значения множеств параметров противодействия атакам путем поиска допустимых вариантов параметров $U^{ДОП}, M_{ПД}^{ДОП}, Z_{ПД}^{ДОП}$. В связи с этим выражение (2) может быть представлено как:

$$P_{УФ}^{КВИС} = F\left[\left(U, M_{ПД}, Z_{ПД}\right)\right], \qquad (5)$$

Методическая схема противодействия компьютерным атакам с целью обеспечения устойчивости функционирования КВИС представлена на рисунке 4.

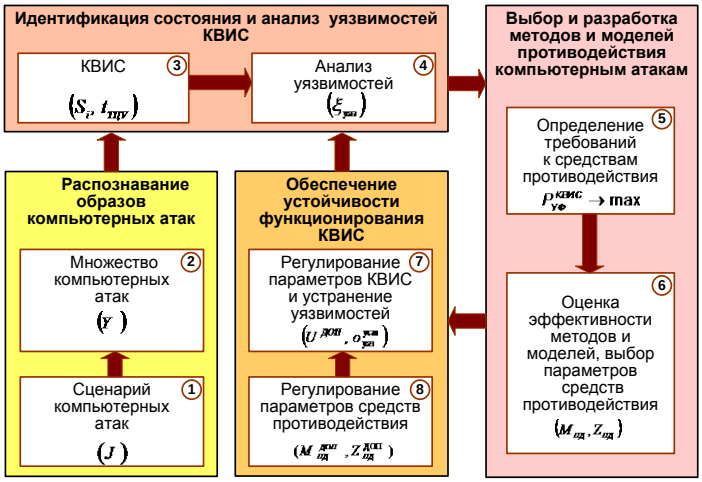

Рисунок 4 – Методическая схема противодействия компьютерным атакам

При разработке методов и моделей противодействия атакам предполагается, что осуществляется противодействие наиболее опасным потенциально возможным атакам, приводящим к нарушению устойчивости функционирования (функциональному поражению) КВИС. Противодействие известным атакам обязательно, а число устраненных неизвестных атак должно стремиться к максимуму.

В КВИС, которые используются для управления транспортом, энергетикой, связью, навигацией и другими промышленными системами и процессами, должен быть реализован принцип «запрещено все то, что не разрешено при выполнении ТЦУ». Этот принцип означает, что на автоматизированных рабочих местах (АРМ) и серверах должно быть установлено только штатное общее и специальное программное обеспечение (ОПО и СПО), в базах данных должна храниться только реальная технологическая информация, должны выполняться только те функции программ, которые определены программной документацией. Нештатные события и непредусмотренные функции, выполняемые в КВИС, подвергаются функциональному и сигнатурному анализу и анализу аномалий на предмет выявления признаков подготовки и проведения потенциальных компьютерных атак.

Таким образом, подход к разработке методов и моделей противодействия компьютерным атакам сведён к выбору допустимых множеств параметров регулирования КВИС, методов, моделей, алгоритмов противодействия атакам и средств предупреждения, обнаружения, анализа компьютерных атак, активного противодействия атакам для достижения максимума обобщенного показателя эффективности противодействия компьютерным атакам, обеспечивающего устойчивость функционирования КВИС.

4 Обобщенный метод распознавания компьютерных атак

Распознавание компьютерных атак в динамике функционирования КВИС представляет собой системный анализ пространства параметров информационно-вычислительного процесса по установленным правилам и выявление тех параметров, которые характеризуют действие атаки. Для системного описания комплекса процедур по противодействию компьютерным атакам в полной мере подходит теория распознавания образов [8, 49, 64], в соответствии с которой объекты компьютерных атак могут быть интерпретированы распознаваемыми образами пространства их признаков.

Компьютерная атака – это образ, который необходимо распознать в процессах сбора, хранения, обработки и передачи информации КВИС при попытках нарушителя интеллектуального вывода его из строя или снижения эффективности применения КВИС. Пространство признаков атак формируется, декомпозируется и систематизируется на основе априорных знаний об опыте эксплуатации КВИС и классификации атак, а затем уточняется по апостериорной информации. Ключевыми средствами и источниками информации для распознавания объектов компьютерных атак и диагностики потенциальных угроз их воздействия на КВИС являются интеллектуальные датчики средств противодействия. Средства противодействия компьютерным атакам совместно со средствами мониторинга состояния информационной безопасности КВИС осуществляют сбор данных от датчиков для формирования пространства признаков атак и оценку возможного нарушения устойчивости функционирования КВИС.

Модель распознавания компьютерных атак на КВИС приведена на рисунке 5.

Словарь признаков компьютерных атак содержит количественные и качественные признаки, которые декомпозируются на:

- детерминированные признаки атак – распознаются сигнатурными методами обнаружения атак;
- вероятностные признаки атак – распознаются методами анализа аномальных отклонений в КВИС;
- логические признаки атак – распознаются методами функционального анализа.

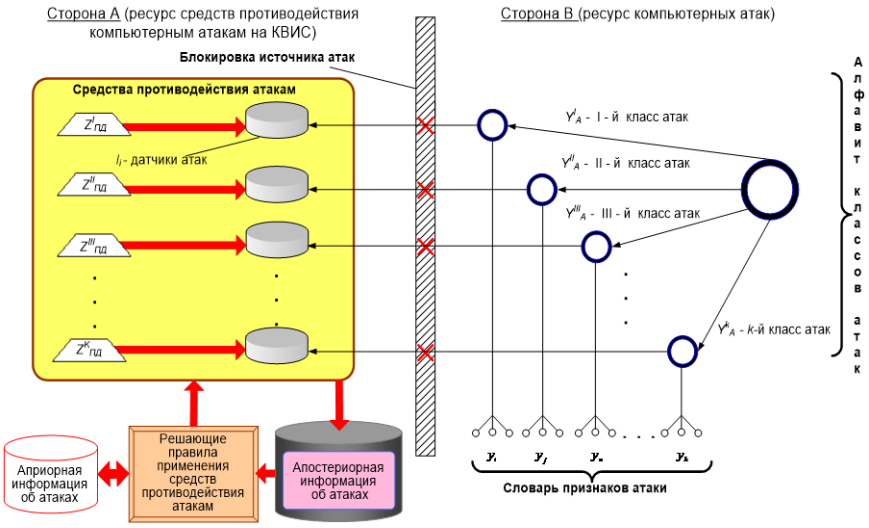

Рисунок 5 – Модель распознавания компьютерных атак на КВИС

Если в модели распознавания априорной информации об компьютерных атаках (эталонной базы данных атак) достаточно для определения решающих правил применения средств противодействия атакам, то используются средства распознавания атак без обучения. Апостериорная информация в модели используется в качестве извещения о необходимости применения средств противодействия на основе использования сигнатурного анализа и анализа аномальных отклонений в КВИС. Если в модели априорной информации недостаточно для решающих правил, то используются средства распознавания атак с обучением. Распознавание атак осуществляется по информации от датчиков, сведениям о мониторинге КВИС, результатах контроля ТЦУ на основе использования функционального анализа.

Ограничением является то условие, что для выработки решающих правил должны быть составлены алфавит классов атак и априорный словарь признаков атак. Если достоверно неизвестен алфавит классов атак, то для КВИС должен быть подготовлен набор решающих правил о принадлежности параметров к определенному классу атак.

Используя материалы [8, 49, 64], допустимо провести аналогию, что при заданном признаковом множестве атак уменьшение числа классов атак приводит к уменьшению ошибок их распознавания, а при увеличении числа классов атак необходимо расширить словарь признаков атак.

Для решения задачи распознавания атак необходимо искать компромисс между размерами алфавита классов атак и объемом рабочего словаря признаков атак на основе

априорной информации о возможных решающих правилах и вычислительных ресурсах КВИС.

Обобщенный метод распознавания компьютерных атак на КВИС определяется математическими соотношениями в следующей последовательности:

1. Определение исходного множества распознаваемых объектов компьютерных атак.

Множество возможных компьютерных атак на КВИС представим как распознаваемые объекты атак для СПКА в виде:

$$\Omega_{YK} = \{\omega_{Y1},...,\omega_{YK}\}, \quad (6)$$

где Ω_{YK} – классы компьютерных атак;

ω_{YK} – объекты компьютерных атак.

2. Разработка априорного алфавита классов компьютерных атак.

Априорный алфавит возможных классов атак и исходное множество распознаваемых объектов атак на КВИС формализуем следующим образом:

$$A_\gamma = \{A_1,...,A_k\}, \bigcup_{j=1}^{g_k} \Omega_{Y_j}^{A_k} = \Omega_Y , \quad (7)$$

где A_i – элементы алфавита классов атак;

j – параметры атак;

g_k – конечное количество подмножеств атак.

Известные классы компьютерных атак формализуются в априорном алфавите классов атак в соответствии с их классификацией [Эл. уч. Техн. осн.]. Неизвестные классы компьютерных атак приводятся в соответствие к известным классам атак путем модификации (уточнения параметров) или формируется самостоятельный класс компьютерных атак.

3. Разработка априорного словаря признаков компьютерных атак.

На основании начальной информации $I_н$ о классах Ω_{Yj}^{Ai} объектов компьютерных атак ω_{Yk} зададим значения признаков компьютерных атак:

$$y_\gamma = \{y_1,...,y_k\}, \quad (8)$$

где y_k – признаки компьютерных атак.

Предположим, что эта совокупность признаков одна и та же для рассматриваемого варианта разбиения возможных классов объектов атак $A\gamma$ при исследовании противодействия компьютерным атакам на конкретный КВИС [1, 4, 28, 31, 51].

4. Описание классов компьютерных атак на языке признаков атак.

Совокупность значений признаков компьютерных атак y_γ позволяет определить описание $I(\omega_Y)$ классов объектов Ω_{Yj}^{Ai} для множества допустимых значений признаков атак $\{0,1\}$, где 0 – означает отсутствие атаки, а 1 – наличие атаки.

Тогда описание классов компьютерных атак имеет вид:

$$I(\omega_y) = [y_1(\omega_y),..., y_k(\omega_{yk})] \qquad (9)$$

Наличие описаний классов атак позволяет определить решающие правила (решающие границы), использование которых обеспечивает минимизацию ошибок при распознавании неизвестных компьютерных атак на КВИС.

5. Декомпозиция множества признаков атак на области в соответствии с классами и алфавитом классов компьютерных атак.

Задача распознавания при описании (9) формулируется как определение вероятности распознавания атак $P_j(\omega_{Yk} \in \Omega_{Yj}^{Ai})$, и функции плотности вероятности распознавания атак $f_{Yj}^{Ai}(y_1,..., y_k)$ для данного объекта ω_{Yk} и набора классов $\Omega_{Y1}^{Ai},...,\Omega_{Ym}^{Ai}$ по обучающей информации $I_н(\Omega_{Y1}^{Ai},...,\Omega_{Ym}^{Ai})$ о классах и описанию объектов атак $I(\omega_Y)$.

Множество возможных решений противодействия атакам по результатам их распознавания определим:

а) условиями декомпозиции множества признаков атак на области:

$$\begin{cases} \forall\, \omega_{Yk} \in \Omega_y = \{\Omega_{Y1}^{A_1},...,\Omega_{Ym}^{A_1}\} \\ I_{\text{н}Ym}^{A_1} \in I_{\text{н}}(\Omega_{Y1}^{A_1},...,\Omega_{Ym}^{A_1}) \\ I(\omega_{Yk}) \in I(\omega_Y),\ V_{Yi} \in V_Y, \\ \exists\ P_j(\omega_Y \in \Omega_{Yj}^{Ai}),\ j = 1, m;\ f_{\Omega_{Yk}}^{A1}(y_1,..., y_k) \end{cases}, \qquad (10)$$

где $\left\{\Omega_{Y1}^{A_1},...,\Omega_{Ym}^{A_1}\right\}$ – набор классов атак;

$I_{\text{н}}\left(\Omega_{Y1}^{A_1},...,\Omega_{Ym}^{A_1}\right)$ – обучающая информация;

V_{Yi} – области на множестве признаков атак;

б) разделяющими функциями, которые позволяют отнести признаки компьютерных атак к соответствующему классу:

$$\begin{cases} \forall y_k \in y_\gamma,\ \Omega_{Y1}^{A_1} = \{\omega_{Y1},...,\omega_{Yi}\},\ \exists F_{Y1}\left(y_{p1},...,y_{pi}\right) \to \max, \\ \qquad \Omega_{Y2}^{A_2} = \{\omega_{Y2},...,\omega_{yj}\},\ \exists F_{Y2}\left(y_{p2},...,y_{pj}\right) \to \max, \\ \qquad ..... \\ \qquad \Omega_{Yk}^{Ak} = \{\omega_{Yk},...,\omega_{YN}\},\ \exists F_{Yk}\left(y_{pk},...,y_{pN}\right) \to \max, \end{cases} \tag{11}$$

где $y_{pk},...,y_{pN}$ – распознанные признаки компьютерных атак, относящиеся к классу атак Ω_{Yk}^{Ak} и обладающие свойством, при котором функция распознавания $F_{Yk}\left(y_{pN}\right)$, стремится к максимуму.

6. Выбор алгоритма распознавания компьютерных атак.

Алгоритм распознавания атак основан на поиске меры близости объекта атаки ω_Y к классу атаки Ω_{Yi}^{Ai}. Как правило, в качестве меры близости используется среднеквадратическое расстояние между данными объекта атаки и совокупность объектов класса атаки [8, 35, 49, 64, 67].

В соответствии с геометрической интерпретацией рисунка 6 алгоритм распознавания компьютерных атак определяется логическими условиями декомпозиции множества признаков атак на классы атак.

Логические условия отнесения признаков объектов компьютерных атак к классам атак $\Omega_{Y1}^{A1},...,\Omega_{Y2}^{A2}$ имеют вид:

$$\begin{cases} \omega_{yi} \in \Omega_{Y1}^{A_1} \left| \left(\rho_{П1}^{y_{p1}}, \rho_{П1}^{y_{p2}}\right) \geq \rho_{П1\text{тр}} \right. \\ \omega_{yj} \in \Omega_{Y2}^{A_2} \left| \left(\rho_{П2}^{y_{p1}}, \rho_{П2}^{y_{p2}}\right) \geq \rho_{П2\text{тр}} \right. \\ \rho_{П1\text{тр}} = \hat{\rho}\left(\Omega_{Y1}^{A_1}\right),\ \rho_{П2\text{тр}} = \hat{\rho}(\Omega_{Y2}^{A_2}), \end{cases} \tag{12}$$

где $\rho_{П1}^{y_{p1}}, \rho_{П1}^{y_{p2}}, \rho_{П2}^{y_{p1}}, \rho_{П2}^{y_{p2}}$ –пороги формирования классов атак;

$\hat{\rho}\left(\Omega_{Y1}^{A1}\right), \hat{\rho}\left(\Omega_{Y2}^{A2}\right)$ – оценки априорных вероятностей распознавания объектов классов атак $\Omega_{Y1}^{A_1}$ и $\Omega_{Y2}^{A_2}$.

Условия объединения объектов компьютерных атак ω_{Yk} в кластер атак (соответствующий классу атак) определяется условным расстоянием между ними по соотношениям [8, 35, 49, 64, 67], а именно:

а) для определения меры близости объекта ω_{Yk} к классу атак Ω_{Ym}^{Ai} по среднеквадратическому расстоянию между данными объекта атаки ω_{Yk} и совокупностью объектов атак $(\omega_{Yk},...,\omega_{Yk+1})$ соответствующего класса Ω_{Ym}^{Ai}:

$$M(\omega_{Yk},\Omega_{Yk}) = \sqrt{\frac{1}{g_k}\sum_{i=1}^{g_k}\rho_{\Pi i}^{YPi^2}(\omega_{Yk},\omega_{Yk+1,i})} \qquad (13)$$

б) для случая, когда признаки компьютерных атак статистически зависимы, расстояние между объектами атак определим по обобщенному расстоянию Махаланобиса:

$$\rho_{\Pi\text{тр}}(\omega_{Yk},\omega_{Yi}) = \sqrt{(y_{pk}-y_{pi})^T \Lambda^T K^{-T}(y_{pk}-y_{pi})\Lambda}\,, \qquad (14)$$

где y_{pk}, y_{pi} – распознанные признаки компьютерных атак;

K^{-T} – ковариационная матрица весовых коэффициентов компьютерных атак, которые определяются по результатам предварительных испытаний на стендовом полигоне и в ходе приемо-сдаточных испытаний КВИС.

Рисунок 6 – Геометрическая интерпретация алгоритма распознавания компьютерных атак

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

На этапе составления рабочего алфавита классов и рабочего словаря признаков компьютерных атак осуществляется уточнение априорной информации (этапы 2, 3 данного метода) с учетом специфики, особенностей применения КВИС и опыта его эксплуатации (или результатов испытаний на стендовом полигоне).

Опыт эксплуатации КВИС [1, 4, 28, 31, 51] и доступная информация об компьютерных атаках [3, 9, 14, 31, 50, 52, 53, 55-57, 63, 65] позволяют сформировать априорный алфавит классов и априорный словарь признаков. Однако на практике объем априорных сведений недостаточен для достоверного выявления атак на множестве признаков атак и необходимо, настраивать СПКА по апостериорной информации об атаках на реальный информационно-вычислительный процесс КВИС.

Основой составления рабочего алфавита классов и рабочего словаря признаков компьютерных атак является использование обучающих средств распознавания компьютерных атак, математическое описание которых имеет следующую последовательность:

а) обучающая выборка задана на основе использования классификации компьютерных атак в виде:

$$\begin{cases} (\omega_{Y1},\ldots,\omega_{Yi}) \in \Omega_{Yi} \\ (\omega_{Yk+1},\ldots,\omega_{Yj}) \in \Omega_{Yj} \\ (\omega_{Yr=1},\ldots,\omega_{Yl}) \in \Omega_{Yl} \\ (\omega_{Yn+1},\ldots,\omega_{Ym}) \in \Omega_{Ym} \end{cases}, \quad (15)$$

где Ω_{Yi} – объекты компьютерных атак – «ложная информация»;

Ω_{Yj} – объекты компьютерных атак – «функциональное поражение»;

Ω_{Yl} – объекты компьютерных атак – «разрыв соединения»;

Ω_{Ym} – объекты компьютерных атак, относящиеся к новому классу неизвестных атак (например, «спам»);

б) при условиях, что априорная вероятность определяется для промежутка времени выполнения ТЦУ и количество объектов атак в каждом классе сравнительно невелико (от 2 до 7), то суммарная оценка априорных вероятностей распознавания объектов каждого из классов известных атак определяется по формуле:

$$\hat{P}(\Omega_Y) = \sum_{i=1}^{k} \hat{P}(\Omega_{Yi}) = \frac{N_i + N_j + N_l + N_m}{N_P}, \quad (16)$$

где N_i, N_j, N_l, N_m – количество объектов атак в каждом из классов;

N_p – общее количество распознаваемых объектов атак.

Кроме того, предполагается, что на основе априорного алфавита признаков атак определены оценки плотности распределения их вероятностей $f_1(x)$,…, $f_m(x)$.

в) неизвестные атаки на основе априорной информации и классификации компьютерных атак определяются по формуле:

$$\overline{P}_{g+1}(\Omega_{Yi}) = \overline{P}_g(\Omega_{Yi}) + \mu_{g+1}\left[\frac{V_{Oi} + K_i^{g+1}}{N_{P+g-1}} - \overline{P}_g(\Omega_{Yi})\right], \quad (17)$$

где $\overline{P}_g(\Omega_{Yi})$ – уточненные оценки g-го шага распознавания атак, полученные на основе априорной информации по результатам отнесения неизвестных атак к соответствующим классам объектов атак;

$1 > \mu_{g+1} > 0$ – коэффициент оценки на $g+1$ - шаге, определенный алгоритмом стохастической аппроксимации функции распознавания атак;

$\overline{P}_{g+1}(\Omega_{Yi})$ – оценка вероятности распознавания неизвестных атак на $g+1$ - шаге;

V_{Oi} – число объектов атак в обучающей выборке;

K_i^{g+1} – число объектов атак, отнесенных к Ω_{Yi} - классу;

г) условия отнесения объектов атак к соответствующим классам определяется соотношением:

$$\Omega_{Yi} = \begin{cases} 1,\ y_i \geq y^*{}_i,\ \omega_i \in \Omega_{Y1} \\ 2, y_j \geq y^*{}_j,\ \omega_j \in \Omega_{Y2} \\ 3, y_l \geq y^*{}_l,\ \omega_l \in \Omega_{Y3} \\ 4, y_m \geq y^*{}_m,\ \omega_m \in \Omega_{Y4} \end{cases}, \qquad (18)$$

где $y_i^*, y_j^*, y_l^*, y_m^*$ – натуральный ряд чисел, определяющий признак атаки;

д) уточненная мера близости атак рабочего алфавита классов и рабочего словаря признаков компьютерных атак определяется путем попарного сравнения объектов неизвестных атак с объектами известных атак. Используя выражения (12 - 15), запишем следующие соотношения:

для эвклидовой меры близости на N-мерном множестве признаков атак справедливо выражение:

$$\rho_n^{yp^2}(\omega_{Yk}, \omega_{Ym}) = \sum_{q=1}^{N} \beta_q \left(y_{pk}^i - y_{pm}^g\right)^2, \qquad (19)$$

где y_{pk}^i – распознаваемые признаки *k*-го объекта *i*-го класса известных атак;

y_{pm}^g – распознаваемые признаки m-го объекта g-го класса неизвестных атак;

$\beta_q = (\beta_1, ..., \beta_N)$ – совокупность признаков объектов атак, принимающих значение 1, если признак атаки определен, и 0, если признак атаки не определен;

для вычисления меры близости по Чебышеву [2, 66, 68] выражение имеет вид:

$$\rho_{\text{п}}^{\text{yp}}(\vec{\omega}_{Yk}, \vec{\omega}_{Ym}) = \max_S \left| y_{kS} - y_{mS} \right|, \qquad (20)$$

где $\vec{\omega}_{Yk}, \vec{\omega}_{Ym}$ – векторы объектов атак, между которыми оценивается расстояние;

y_{kS} – S-я составляющая вектора $\vec{\omega}_{Yk}$;

y_{km} – S-я составляющая вектора $\vec{\omega}_{Ym}$.

Меры близости между объектами пар классов атак Ω_{yi} и Ω_{yg}, Ω_{yj} и Ω_{yg}, Ω_{yl} и Ω_{yg} определены по среднеквадратическим разбросам объектов классов атак:

$$\begin{cases} M^*\left(\Omega_{Yi}, \Omega_{Yg}\right) = \sqrt{\frac{1}{k_i}\frac{1}{k_g}\sum_{i=1}^{k_i}\sum_{m=1}^{k_g}\sum_{q=1}^{N}\beta_q\left(y_{pi}^{i} - y_{pm}^{g}\right)^2} \\ M^*\left(\Omega_{Yj}, \Omega_{Yg}\right) = \sqrt{\frac{1}{k_j}\frac{1}{k_g}\sum_{j=1}^{k_j}\sum_{m=1}^{k_g}\sum_{q=1}^{N}\beta_q\left(y_{pj}^{j} - y_{pm}^{g}\right)^2} \\ M^*\left(\Omega_{Yl}, \Omega_{Yg}\right) = \sqrt{\frac{1}{k_l}\frac{1}{k_g}\sum_{l=1}^{k_l}\sum_{m=1}^{k_g}\sum_{q=1}^{N}\beta_q\left(y_{pl}^{l} - y_{pm}^{g}\right)^2} \end{cases}, \quad (21)$$

где i=1,…,ki; j=1,…,kj; l=1,…,kl; m=1,…, kg;

е) условия достаточности рабочего алфавита классов и рабочего словаря признаков компьютерных атак для успешного противодействия атакам определим соотношениями:

$$\begin{cases} \forall A_{\gamma p} = \sum_{i=1}^{k} A_{ip}, \; C_{\text{т}} = C_{Tp}, \; T_{ТЦУ} = T_{Треб}; \\ \exists \Omega_{Yp} = \sum_{j=1}^{g_k} \Omega_{Ypj}^{A_k}, \; F_A\left(A_{\gamma p} \bigcup A_{\gamma}\right) \to \max, \\ F_{\Omega}\left(\Omega_Y \bigcup \Omega_{yp}\right) \to \max, \\ A_{\gamma p} : \Omega_{Yj}^{A_j} \bigcup \Omega_{Ypj}^{A_k} = \Omega_Y, \; F_{\Omega_Y}^{A_j}\left[P\left(\Omega_Y \middle| y_i\right)\right] \to \max \end{cases}, \quad (22)$$

где $A_{\gamma p}$ – рабочий алфавит классов атак;

Ω_{Yp} – рабочие классы атак;

F_A – функция, построенная на основе данных пересечения множеств априорного и рабочего алфавитов классов атак;

F_{Ω} – функция, построенная на основе данных пересечения множеств рабочих и априорных классов атак;

$F_{\Omega_Y}^{A_i}\left[P\left(\Omega_Y \middle| y_i\right)\right]$ – функция выигрыша от распознавания объектов атак класса Ω_Y на основе априорной вероятности правильного решения задачи распознавания по возможным значениям признаков атак y_j.

Ограничения рабочего алфавита классов и рабочего словаря признаков компьютерных атак состоят в следующем:

– наличие технической возможности разработки датчиков, которые обеспечивают распознавание признаков компьютерных атак;
– учет затрат на разработку средств распознавания при их реализации в составе СПКА и при модернизации КВИС;
– допустимый объем временных и вычислительных ресурсов на выполнение ТЦУ, накладывающий ограничения на период времени выявления атак, возможное количество датчиков атак и загрузку сетевого трафика КВИС;
– погрешность безошибочного, достоверного и точного распознавания объектов компьютерных атак.

8. Выбор критериев распознавания компьютерных атак. Этот выбор заключается в следующем:

– определение критерия распознавания компьютерных атак – вероятности правильного распознавания атак при ограничениях ТЦУ на сбор, хранение, обработку и передачу информации по формуле:

$$\begin{cases} \overline{P}_{PAi}\left(\Omega_{Yi}^{Ai} \middle| y_i\right) \geq P_{\text{Треб}i} \\ \overline{P}_{PAj}\left(\Omega_{Yj}^{Aj} \middle| y_j\right) \geq P_{\text{Треб}j} \\ \overline{P}_{PAl}\left(\Omega_{Yl}^{Al} \middle| y_l\right) \geq P_{\text{Треб}l} \\ \overline{P}_{PAg}\left(\Omega_{Yg}^{Ag} \middle| y_g\right) \geq P_{\text{Треб}g} \end{cases}, \qquad (23)$$

где $\overline{P}_{PAi}$, $\overline{P}_{PAj}$, $\overline{P}_{PAl}$, $\overline{P}_{PAg}$ – оценки вероятности правильного распознавания атак, усредненные по временным значениям признаков рабочего словаря, описываемого векторами признаков атак y_i, y_j, y_l, y_g соответственно;

– определение ограничения на стоимость создания датчиков распознавания компьютерных атак по формуле:

$$\sum_{i=1}^{N} \lambda_{Yi} C_{li} \leq C_{\text{Треб}}, \qquad (24)$$

где λ_{Yi} – решающее правило по определению атак в соответствии со словарем признаков;

C_{li} – стоимость создания аппаратно-программных датчиков распознавания атак;

$C_{\text{Треб}}$ – требуемая стоимость на создание датчиков, в рамках которой должны быть ограничены затраты;

– определение критерия эффективности распознавания компьютерных атак средствами противодействия при учете ограничения (23) производится по формуле:

$$G_P = \sum_{i=1}^{m}\sum_{j=1}^{k} P_{PAi}\left(\Omega_{\text{Yi}}^{Ai}\middle| y_i\right) F\left(\Omega_{Yj}^{Aj}\right), \qquad (25)$$

где i=1, …, m – количество возможных классов атак;

j=1, …, k – количество возможных объектов атак;

$F\left(\Omega_{Yj}^{Aj}\right)$ – функция выигрыша от возможных решений по распознаванию объектов атак ω_{Yk}, отнесенных к алфавиту классу атак Ω_{Yj}^{Aj}.

9. Формирование ограничений на распознавание атак выполняется следующим образом:

– условия отнесения компьютерных атак к множеству признаков атак, на котором осуществляется поиск средствами противодействия, записывается в виде:

$$\begin{cases} 0, & y_{\text{m}} \le \rho_{\text{п1}} \quad \text{– нет атаки} \\ 1, & y_{\text{m}} \ge \rho_{\text{п2}} \quad \text{– есть атака} \\ \dfrac{1}{v_{\,K\,KBИС}}, & \rho_{\text{п3}} \le y_{\text{m}} \le \rho_{\text{п4}} \quad \text{–"ложное" обнаружение атак} \end{cases}, \qquad (26)$$

где $\rho_{п1}$, $\rho_{п2}$, $\rho_{п3}$, $\rho_{п4}$ – числа, характеризующие пороги срабатывания датчиков распознавания атак;

$v_{КВИС\,i}$ – решающее правило для защищаемой КВИС;

– объем обучающей информации, используемой при корректировке рабочего алфавита классов и рабочего словаря признаков компьютерных атак, ограничен возможностями таблицы обучения принадлежности к классам компьютерных атак (таблица 1).

Таблица 1 – Решающая выборка обучения принадлежности распознаваемых объектов к классам компьютерных атак

Признаки компьютерных атак и их значения				Объекты атак	Классы атак
y_i	y_j	y_l	y_m		
$\alpha_{1,i},...,\alpha_{1,i+1}$				ω_{Y1} … ω_{Yi}	Ω_{Yi}
	$\alpha_{2,j},...,\alpha_{2,j+1}$			ω_{Yk+1} … ω_{Yj}	Ω_{Yj}
		$\alpha_{3,l},...,\alpha_{3,l+1}$		ω_{Yr+1} … ω_{Yl}	Ω_{Yl}
			$\alpha_{4,g},...,\alpha_{4,g+1}$	ω_{Yn+1} … ω_{Ym}	Ω_{Yg}

10. Минимизация ошибок «ложного» обнаружения компьютерных атак и ошибок не распознавания неизвестных атак по критериям Неймана-Пирсона и Байеса.

Процедура определения результатов обнаружения и распознавания компьютерных атак по фактам срабатывания датчиков средств противодействия компьютерным атакам по критерию Неймана-Пирсона представлена на рисунке 7. На этапах обнаружения и распознавания признаков компьютерных атак допускаются ошибки первого и второго рода: «ложного» обнаружения атак и не распознавания неизвестных компьютерных атак. На основе анализа рисунка 7 получим выражения для вероятностей «ложного» обнаружения компьютерных атак и не распознавания неизвестных атак, имеющие вид:

$$\begin{cases} P_2 = 1 - P_1;\ \ \overline{\alpha}_0 = 1 - \alpha_0;\ \ \overline{\beta}_0 = 1 - \beta_0;\ \ \overline{\beta}_P = 1 - \beta_P, \\ P_{OA} = P_2\overline{\beta}_0\overline{\beta}_P; P_{PA} = P_1\alpha_0\overline{\beta}_p; P_{HPA} = P_2\overline{\beta}_0\beta_p, \\ P_{HOHPA} = P_1\alpha_0\beta_0; P_{HOA} = P_2\beta_0; P_{OOA} = P_1\overline{\alpha}_0, \end{cases} \quad , \qquad (27)$$

где P_1 – вероятность отсутствия атаки;

P_2 – вероятность воздействия атаки на КВИС;

α_0 – ошибка первого рода - условная вероятность «ложного» обнаружения компьютерных атак;

β_0, β_P – ошибки второго рода - условные вероятности не распознавания неизвестных компьютерных атак;

P_{OA} – вероятность обнаружения компьютерных атак;

P_{PA} – вероятность распознавания отсутствия компьютерных атак;

P_{HPA} – вероятность не распознавания неизвестных компьютерных атак;

P_{HOHPA} – вероятность не обнаружения и не распознавания неизвестных компьютерных атак;

P_{HOA} – вероятность не обнаружения компьютерных атак;

P_{OOA} – вероятность обнаружения отсутствия компьютерных атак.

На этапе обнаружения компьютерных атак с условной вероятностью $\overline{\beta_0}$ происходит обнаружение компьютерных атак и с ошибкой второго рода $\beta_0 = 1 - \overline{\beta_0}$ не обнаружение атак. В случае отсутствия атак Y_A^* с условной вероятностью $\overline{\alpha_0}$ они не обнаруживается и с ошибкой первого рода α_0 происходит их «ложное» обнаружение. На этапе распознавания компьютерных атак имеется ошибка распознавания второго рода $\beta_P = 1 - \overline{\beta_P}$.

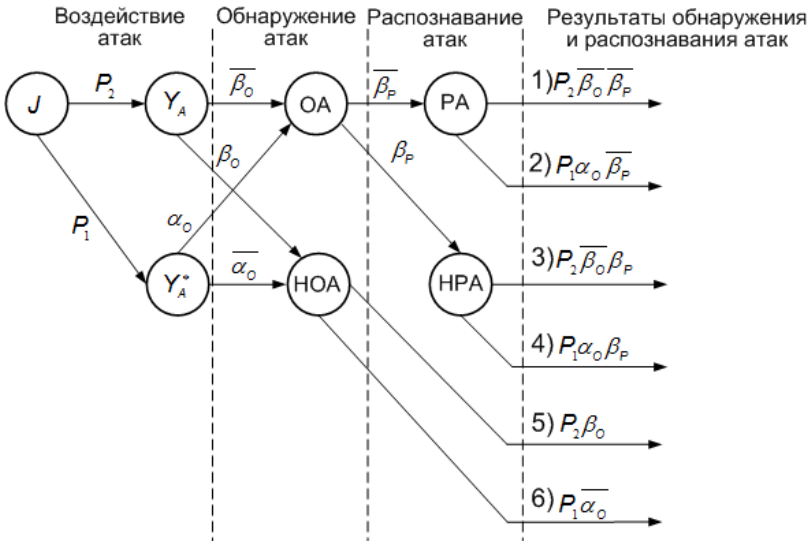

Рисунок 7 – Граф определения результатов обнаружения и распознавания атак

Обозначения на рисунке 7:

Y_A – наличие атаки; Y_A^* – отсутствие атаки;

ОА – обнаружена атака; НОА – не обнаружена атака;

РА – распознана атака; НРА – не распознана атака.

Наихудшие результаты обнаружения и распознавания атак соответствуют 3-му и 5-му результатам на рисунке 7. Третий результат соответствует событиям, когда атаки воздействуют на КВИС, и они обнаружены с условной вероятностью $\overline{\beta_{\text{О}}}$, но не распознаны с ошибкой второго рода $\beta_{\text{Р}}$. Для уменьшения ошибок не распознавания неизвестных атак используется не линейная функция распознавания $F_{н}(y_1,y_2)$ на основе рабочего алфавита классов атак и обучающей выборки, которая устраняет ошибки распознавания при использовании линейной функции распознавания $F_{л}(y_1,y_2)$ на основе априорного алфавита классов атак.

На рисунках 8а и 8б приведены иллюстрации линейной и нелинейной функций распознавания при анализе пространства компьютерных атак на основе двух признаков атак y_1, y_2. На этих рисунках символом $\oplus$ обозначены признаки атак класса Ω_{y1}, а символом $\otimes$ обозначены признаки атак класса Ω_{y2}.

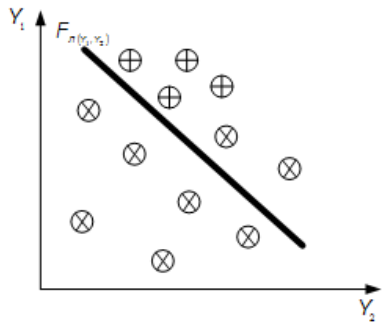

Рисунок 8а – Иллюстрация ошибок не распознавания неизвестных атак при использовании линейной функции распознавания и априорного алфавита классов атак

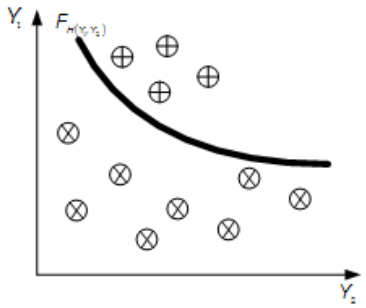

Рисунок 8б – Иллюстрация ошибок не распознавания неизвестных атак при использовании не линейной функции распознавания и рабочего алфавита классов атак с учетом обучающей выборки

Пятый результат оценивается вероятностью не обнаружения атак, которую можно уменьшить путем максимального сдвига порога классификации y_0 вправо (рисунок 9).

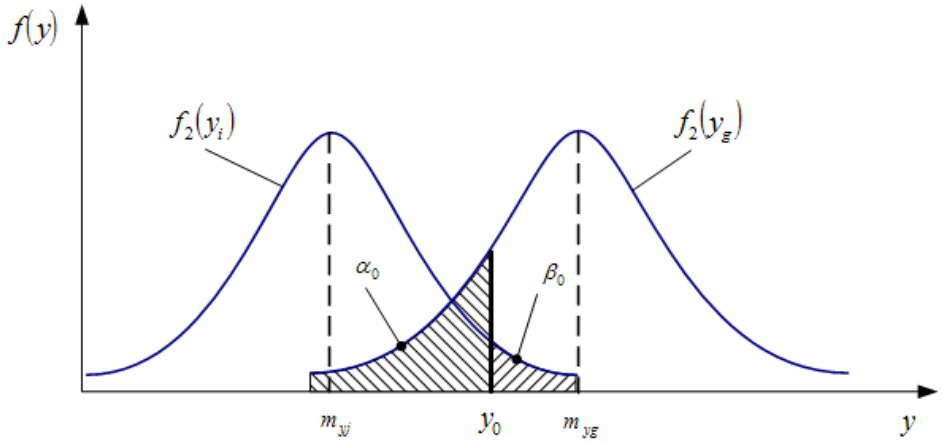

Рисунок 9 – Графические зависимости плотности распределения вероятности распознавания компьютерных атак

В соответствии с критерием Неймана-Пирсона [11-13, 37, 57, 62, 68] и графическими зависимостями плотности распределения вероятности распознавания компьютерной атаки (рисунок 9), а также классификацией атак условие минимизации ошибок обнаружения и распознавания атак запишем в виде:

$$\begin{cases} \forall P_{Л} = const,\ \exists P_{H1} = \min\limits_{y_{oi} y_{og}} \left[P_2 \left(1 - \int\limits_{y_{oi}}^{\infty} f_2(y_i) dy \int\limits_{y_{og}}^{\infty} f_2(y_g) dy \right) \right] \\ \exists P_{H2} = \min\limits_{y_{oj} y_{og}} \left[P_2 \left(1 - \int\limits_{y_{oj}}^{\infty} f_2(y_j) dy \int\limits_{y_{og}}^{\infty} f_2(y_g) dy \right) \right] \\ \exists P_{H3} = \min\limits_{y_{ol} y_{og}} \left[P_2 \left(1 - \int\limits_{y_{ol}}^{\infty} f_2(y_l) dy \int\limits_{y_{og}}^{\infty} f_2(y_g) dy \right) \right] \end{cases} . \quad (1.28)$$

Минимизация ошибок «ложного» обнаружения компьютерных атак и ошибок не распознавания неизвестных атак по критерию Байеса осуществляется исходя из следующих предположений.

Предположим, что весь набор возможных решений сводится к бинарному решению отнесения ошибок обнаружения атак к одному из двух классов: ошибок «ложного»

обнаружения компьютерных атак и ошибок не распознавания неизвестных атак. Пусть возможны случайные события:

y – обнаружения атаки и отнесение к алфавиту классов атак Ω_{Yj} с вероятностью $P(y)$;

α_k – «ложного» обнаружения компьютерных атак с вероятностью $P(\alpha_k)$;

β_k – «не выявления» (пропуска) неизвестных атак по результатам мониторинга защищенности и устойчивости функционирования КВИС.

Тогда в соответствии с критерием Байеса условные вероятности того, что произойдет событие α_k, при условии, что произошло событие y, и условные вероятности того, что произойдет событие β_k, при условии, что произойдет событие y, имеет вид:

$$P(\alpha_k / y) = \frac{P(\alpha_k)P(y/\alpha_k)}{\sum_j P(\alpha_j)P(y/\alpha_j)}, \quad (29)$$

$$P(\beta_k / y) = \frac{P(\beta_k)P(y/\beta_k)}{\sum_j P(\beta_j)P(y/\beta_j)}, \quad (30)$$

где $P(y/\alpha_k)$, $P(y/\alpha_j)$, $P(y/\beta_k)$, $P(y/\beta_j)$ – плотности условных вероятностей.

В соответствии с центральной предельной теоремой для большой выборки компьютерных атак принимается гипотеза о нормальном законе функции плотности распределения вероятности. Тогда условная вероятность безошибочного распознавания атак и отнесения их к соответствующему классу атак имеет вид:

$$P_{БОШ}(\Omega_Y | y_i) = \frac{1}{\sigma_i\sqrt{2\pi}} e^{\left[-\frac{1}{2}\left(\frac{y-m_{yi}}{\sigma_i}\right)^2\right]}, \quad (31)$$

где σ_i – среднеквадратическое отклонение случайной величины y_i;

m_{yi} – математическое ожидание случайной величины y_i.

Решающее правило по отнесению вектора параметров неизвестных атак Y_{pm}^{g} m-го объекта g-го класса атак к одному из известных классов Ω_{Yj} на j-м шаге работы средств

противодействия компьютерным атакам в соответствии с критерием Байеса запишем в виде:

$$P(\Omega_{Yj})P(\overline{Y}^{g}_{pm}/\Omega_{Yj}) \geq P(\Omega_{Yk})P(\overline{Y}^{g}_{pm}/\Omega_{Yk}), \qquad (32)$$

где $P(\Omega_{Yj})$ – вероятность отнесения атаки к классу известных атак Ω_{Yj};

$P(\overline{Y}^{g}_{pm}/\Omega_{Yj})$ – плотность условной вероятности отнесения выявленной атаки к известному классу атак Ω_{Yj};

$P(\Omega_{Yk})$ – вероятность отнесения атаки к классу неизвестных атак Ω_{Yk};

$P(\overline{Y}^{g}_{pm}/\Omega_{Yk})$ – плотность условной вероятности отнесения выявленной атаки к неизвестному классу атак Ω_{Yk}.

На основе критерия Байеса среднее значение цены риска принятия решения по отнесению вектора параметров неизвестных атак $\overline{Y}^{g}_{pm}$ к классу атак Ω_{Yk} имеет вид:

$$\mu_{P}(D_i/\overline{Y}^{g}_{pm}) = \sum_{j=1}^{\gamma} c(D_i/\Omega_{Yk})P(\Omega_{Yk}/\overline{Y}^{g}_{pm}) \quad , \qquad (33)$$

где D_i – решающее правило, по которому вектор атаки $\overline{Y}^{g}_{Pm}$ принадлежит классу Ω_{Yk};

$c(D_i/\Omega_{Yk})$ – условная цена принятия решения D_i;

$P(\Omega_{Yk}/\overline{Y}^{g}_{pm})$ – условная вероятность того, что $\overline{Y}^{g}_{pm}$ отнесен к классу Ω_{Yk}.

В качестве примера, когда возможные решения по отнесению компьютерных атак $\overline{Y}^{g}_{pm}$ сводятся к принятию решения по классификации атак на два класса Ω_{Y1} и Ω_{Y2}.

С использованием критерия Байеса решающее правило записывается соотношением:

$$\frac{P(\overline{Y}^{g}_{pm}/\Omega_{Y1})}{P(\overline{Y}^{g}_{pm}/\Omega_{Y2})} \geq \frac{P(\Omega_{Y2})}{P(\Omega_{Y1})}, \qquad (34)$$

где $P\left(\overline{Y}_{pm}^{g}/\Omega_{Y1}\right)$ и $P\left(\overline{Y}_{pm}^{g}/\Omega_{Y2}\right)$ – плотности условных вероятностей отнесения атаки $\overline{Y}_{pm}^{g}$ к классам Ω_{Y1} и Ω_{Y2} соответственно.

Графическая иллюстрация для принятия решения по отнесению вектора параметров атак $\overline{y}_{pm}^{g}$ при двух классах атак Ω_{Y1} и Ω_{Y2} в соответствии с формулой (34) приведена на рисунке 10.

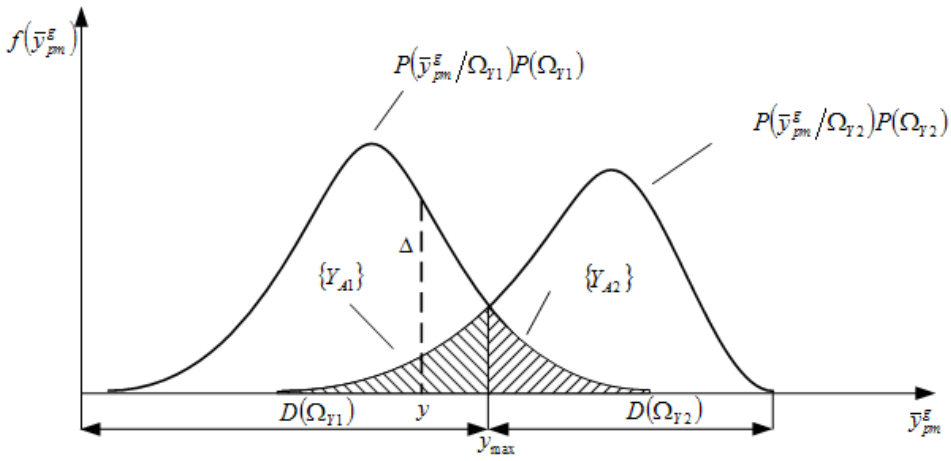

Рисунок 10 – График для принятия решения по отнесению вектора параметров атак $\overline{y}_{pm}^{g}$ при двух классах атак Ω_{Y1} и Ω_{Y2}

На рисунке 10 представлены две графические зависимости для условных вероятностей отнесения $\overline{y}_{pm}^{g}$ к одному из классов атак Ω_{Y1} и Ω_{Y2}, по которым определяются ошибки отнесения параметров атак по классам, исходя из следующих соображений:

1. При делении множества y_{pm}^{g} на два подмножества $\{Y_{A1}\}$ и $\{Y_{A2}\}$ линией Δ выполняются условия:

$\forall y_{pm}^{g} < y \rightarrow \exists\ y \in \Omega_{Y1}$,

$\forall y_{pm}^{g} < y \rightarrow \exists\ y \in \Omega_{Y2}$,

$D(\Omega_{Y1})$, $D(\Omega_{Y2})$ – цены принятия решения.

2. Для класса атак Ω_{Y1} подмножество $\{Y_{A1}\}$ является областью «ложного» обнаружения компьютерных атак, а подмножество $\{Y_{A2}\}$ считается областью не распознавания неизвестных атак.

3. Для класса атак Ω_{Y2} подмножество $\{Y_{A2}\}$ является областью «ложного» обнаружения компьютерных атак, а подмножество $\{Y_{A1}\}$ считается областью не распознавания неизвестных атак.

4. На линии, обозначенной $y_{\max}$, при бинарной оценке решений по отнесению атак y_{pm}^{g} к классам Ω_{Yi} достигается максимально правдоподобное решение по классификации атак.

Достижение устойчивости функционирования КВИС определяется конечным числом решений по выполнению ТЦУ (совокупности процессов сбора, обработки и передачи информации на заданном интервале времени). Сохранение заданных требований по устойчивости функционирования КВИС в условиях воздействия атак зависит от степени детализации распознавания атак, наибольшее значение которой будет, если количество классов распознавания атак равно конечному количеству возможных решений по противодействию им. Другим важным фактором сохранения эффективности информационно-вычислительных процессов КВИС в условиях атак является точность решения задачи распознавания атак – чем она выше, тем меньше вероятность не обнаружения атак или «ложного» обнаружения атак.

При заданном словаре признаков компьютерных атак увеличение алфавита классов атак уменьшает точность решения задачи их распознавания. Увеличение словаря признаков компьютерных атак приводит к существенному усложнению датчиков СПКА, алгоритмов распознавания, и следовательно к увеличению затрат на разработку СПКА и КВИС.

Таким образом, обобщенный метод распознавания компьютерных атак на КВИС отличается от известных введением логических условий для распознавания образов компьютерных атак и дополнительных математических соотношений для минимизации ошибок «ложного» обнаружения атак и ошибок не распознавания неизвестных атак по критериям Неймана-Пирсона и Байеса.

5 Алгоритм динамических процессов противодействия компьютерным атакам на КВИС

Средства противодействия компьютерным атакам на КВИС должны обнаруживать и устранять атаки за минимальное время (секунды) для обеспечения резерва времени на восстановление КВИС (от нескольких минут до десятков минут) и поддержания устойчивости функционирования на заданном уровне.

Алгоритм динамических процессов противодействия компьютерным атакам на КВИС можно представить совокупностью процессов регулирования:

- информационно-вычислительных ресурсов КВИС;
- управляющей информации по выполнению ТЦУ;
- параметров СПКА и средств администрирования КВИС;
- параметров активного противодействия компьютерным атакам.

Алгоритм динамических процессов противодействия компьютерным атакам на КВИС, являющийся базовой структурой управления противодействием атакам и обеспечения устойчивости функционирования КВИС на основе регулирования его процессов, представлен на рисунке 11.

Информационные потоки, циркулирующие в КВИС в условиях воздействия компьютерных атак, включают в свой состав следующие виды информации:

- информация контроля информационно-вычислительных ресурсов КВИС (процессы обеспечения устойчивости функционирования КВИС);
- управляющая информация по выполнению ТЦУ (процессы обеспечения устойчивости функционирования КВИС);
- информация регулирования СПКА по извещению датчиков и администрирования КВИС (процессы предупреждения, обнаружения, анализа атак);
- информация регулирования параметров активного противодействия средствам нарушителя (процессы активного противодействия атакам).

Регулирование процессов в КВИС в условиях воздействия компьютерных атак отражает динамику перехода КВИС из одного состояния в другое вследствие регулирования его параметров и регламентов обработки данных при выполнении ТЦУ.

Применение алгоритма динамических процессов противодействия компьютерным атакам осуществляется следующим образом (рисунок 11).

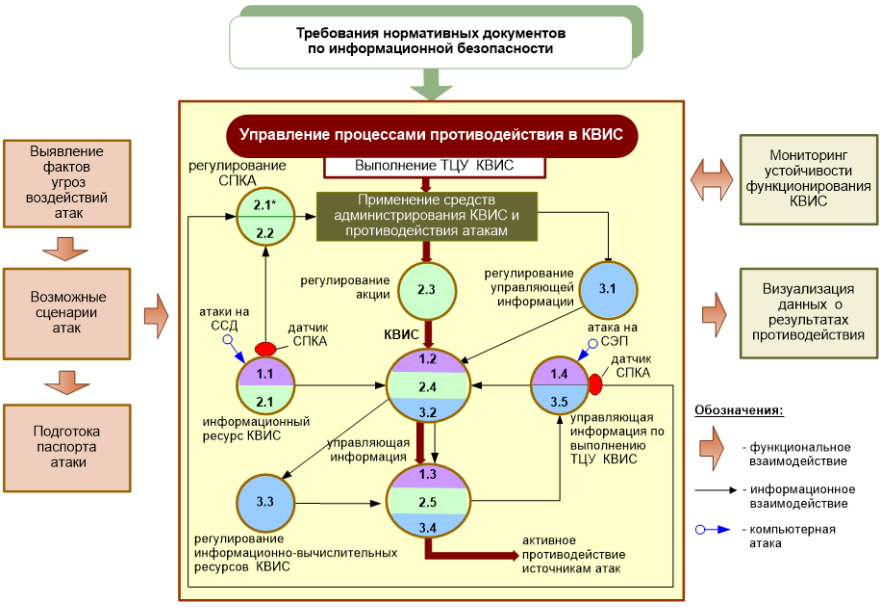

Рисунок 11 – Алгоритм динамических процессов противодействия компьютерным атакам на КВИС

Шаги 1.1 – 1.4. Штатное выполнение ТЦУ в КВИС (регулирование информационно-вычислительных ресурсов).

Первоначальной стадией работы алгоритма является формирование информационного ресурса КВИС на основе сбора входных данных, поступления их по каналам связи и размещения в базах данных КВИС. Далее на основе подготовки исходных данных и проведения вычислений по расчетным программам осуществляется подготовка управляющей информации. Конечной стадией управления является доставка управляющей информации по выполнению ТЦУ на объект управления и ввод данных в исполнительное устройство. В целом штатное выполнение ТЦУ в КВИС характеризуется оптимальным использованием информационно-вычислительных ресурсов КВИС и нахождением системы в одном из состояний выполнения ТЦУ.

Шаги 2.1 (2.1*) – 2.5. Воздействие (предупреждение воздействия) компьютерных атак на КВИС, противодействие атакам путем регулирования параметров СПКА и администрирования КВИС (процессы предупреждения, обнаружения, анализа атак), выполнение активного противодействия компьютерным атакам нарушителя.

Изначально воздействие компьютерных атак может быть оказано следующими способами:

- воздействие, скрытое в получаемых входных данных КВИС (например, атака «ложная информация» на сервер сбора данных – атака на ССД);
- воздействие на протоколы передачи данных (атака «разрыв соединения» в СЭП);
- воздействие, заключающееся в инициировании условий срабатывания закладных программных (программно-аппаратных) элементов (недекларированных возможностей).

Кроме того, атака может производиться и на протоколы передачи данных (атака на сервер электронной почты), в том числе и при выдаче управляющей информации непосредственно для реализации управляющего воздействия на объект.

В случае воздействия компьютерной атаки на ресурс КВИС (подготовки воздействия путем сканирования уязвимостей КВИС), предполагается, что будет два варианта реакции КВИС:

1. Факты подготовки компьютерных атак будут выявлены (предупреждение угроз воздействий атак – 2.1*) на основе анализа признаков потенциальных угроз компьютерных атак с использованием их классификации и результатов работы традиционных средств защиты информации и администрирования безопасности информации.

2. Воздействие будет зафиксировано датчиками СПКА.

Первый вариант реакции КВИС – заключается в предупреждении атаки на основе регулирования СПКА путем дополнительной настройки ее параметров, средств администрирования безопасности информации и устранения уязвимостей КВИС (исправления ошибок в СПО, установки дополнительных средств защиты информации и проведения организационно-технических мероприятий).

Второй вариант реакции КВИС – в результате срабатывания датчиков СПКА компьютерная атака обнаруживается и далее осуществляется регулирование СПКА по детальному анализу атаки и заполнению паспорта атаки [Эл. уч. Техн. осн.].

Затем выполняется регулирование параметров активного противодействия средствам нарушителя (планирование мероприятий, выбор средств противодействия), осуществляется необходимая настройка КВИС, реализуется активное противодействие средствам нарушителя (блокирование источника атаки, перенаправление атаки на ложные объекты) и визуализируются данные оператору о результатах противодействия.

Шаги 3.1 – 3.5. Мониторинг устойчивости функционирования (регулирование управляющей информации).

Воздействия атак на КВИС в лучшем случае приводят к задержке выполнения ТЦУ, а в худшем, могут привести к функциональному поражению КВИС. Восстановление устойчивости функционирования КВИС происходит путем регулирования управляющей информации в КВИС с учетом задержек на восстановление искаженной информации, перезапуск программ и аппаратно-программных комплексов, восстановление вычислений по контрольным точкам и других процедур по восстановлению работоспособности КВИС. После завершения процессов восстановления осуществляется стадия выдачи управляющей информации по выполнению ТЦУ на объект управления и исполнительное устройство. В дальнейшем производится оценка показателей устойчивости функционирования, нанесенного ущерба от атак, и КВИС переходит в состояние штатных процедур обработки информации, определенных ТЦУ.

Следует отметить, что в алгоритме заложен такой подход к регулированию процессов в КВИС, при котором с наивысшим приоритетом осуществляется выполнение ТЦУ (без снижения качества ниже допустимого уровня и срыва времени выполнения технологических операций). Сохранение устойчивости функционирования КВИС особенно важно в критические периоды обработки данных. В соответствии с подготовленными средствами противодействия атакам производится регулирование и корректировка ТЦУ и в динамике его выполнения реализуется активное противодействие средствам нарушителя.

Алгоритм динамических процессов противодействия компьютерным атакам на КВИС по своей сути представляет совокупность событий, происходящих по определенным условиям и переводящим систему из одного состояния в другое после соответствующих регулировок.

Таким образом, алгоритм динамических процессов противодействия компьютерным атакам на КВИС формализован в виде процессов регулирования информационно-вычислительных ресурсов и управляющей информации КВИС, процессов регулирования СПКА и активного противодействия средствам нарушителя, являющийся основой управления противодействием компьютерным атакам.

6 Идентификация состояния КВИС на основе модели динамических процессов противодействия компьютерным атакам

Модель динамических процессов противодействия компьютерным атакам в соответствии с теорией автоматического управления можно представить стохастической управляемой системой, описываемой уравнением в форме Ланжевена с аддитивным белым шумом [61]. Под аддитивным белым шумом будем понимать вектор компьютерных атак на КВИС.

Указанная модель характеризуется следующей последовательностью.

1. Идентификация состояния динамического процесса функционирования КВИС в условиях воздействия компьютерных атак описывается уравнением:

$$S^P = f\left(S, U, T_{ПД}\right) + \eta\left(t_д\right);\ T_{ПД} = t_д + t_p + t_{АП}, \qquad (35)$$

где $S = \left(s_1, s_2, ..., s_i\right)$ – вектор состояний КВИС;

$U = \left(u_1, u_2, ..., u_k\right)$ – вектор регулирования (управления) КВИС;

$T_{ПД}$ – время противодействия атакам;

$t_д$ – время действия атаки;

t_p – время реакции КВИС и СПКА на атаку (процессы предупреждения, обнаружения, анализа атак средствами СПКА и администрирования СЗИ КВИС);

$t_{АП}$ – время активного противодействия средствам нарушителя;

$\eta\left(t_д\right)$ – q-мерный случайный возмущающий процесс (действия компьютерных атак) с нулевым математическим ожиданием $M\left[\eta\left(t_д\right)\right] = 0$ и ковариационной матрицей вида:

$$\mathrm{E}[\eta(t_д)\eta^T(t_p)] = Q\left(t_д\right)\delta\left(t_p - t_д\right),$$

где «T» – символ транспонирования;

$\delta(t_p - t_\partial)$ - непрерывная функция, определенная в подпространствах состояний устойчивости функционирования КВИС.

Пространство состояний S^P является конечномерным вектором состояний динамических процессов функционирования КВИС, определяемых ТЦУ.

2. Определение дискретной последовательности моментов времени противодействия атакам:

$$T_{ПД} = \left\{ t_{ПД0}, t_{ПД1}, ... t_{ПДК-1}, t_{ПДК}, t_{ПДК+1} \right\}, \quad (36)$$

Для наглядного представления динамических процессов функционирования КВИС в условиях воздействия компьютерных атак и выявления закономерностей в порядке регулирования КВИС и СПКА контур управления КВИС формализован алгоритмом динамических процессов регулирования КВИС (рисунок 12).

Предполагается, что регулирование процессов функционирования КВИС в условиях воздействия компьютерных атак осуществляется на основе использования априорной информации о характеристиках КВИС, СПКА, известных компьютерных атаках и знаний об ограничениях выполнения ТЦУ. Однако на практике для решения задачи автоматизированного управления КВИС в условиях воздействия компьютерных атак необходимо заранее оценить параметры КВИС и СПКА по экспериментальным данным на стендовом полигоне (идентификация КВИС в терминах теории автоматического управления) с целью обеспечения устойчивости функционирования КВИС.

На рисунке 12 управление противодействием компьютерным атакам на КВИС обеспечивается путем устранения ошибок управления при выполнении каждого режима функционирования КВИС и соответствующих процессов регулирования:

- устранение ошибки управления внутренними параметрами КВИС ΔR путем регулирования информационно-управляющих ресурсов;
- устранение ошибки выходных данных ΔU за счет использования вектора управляющих воздействий и регулирования управляющей информации по выполнению ТЦУ;
- устранение ошибки управления на основе использования методов, моделей и алгоритмов противодействия компьютерным атакам $\Delta M_{ПД}$ путем введения дополнительных функций регулирования параметров СПКА и средств

администрирования КВИС;

– устранение ошибки управления на основе применения средств противодействия компьютерным атакам $\Delta Z_{ПД}$ путем регулирования параметров СПКА и средств активного противодействия источникам атак.

Поиск решений по управлению стохастической системой в пространстве ее возможных состояний производится в детерминированной постановке, при которой реализуется принцип разделения для нелинейных систем – управление и идентификация параметров для подпространств с детерминированными условиями применения.

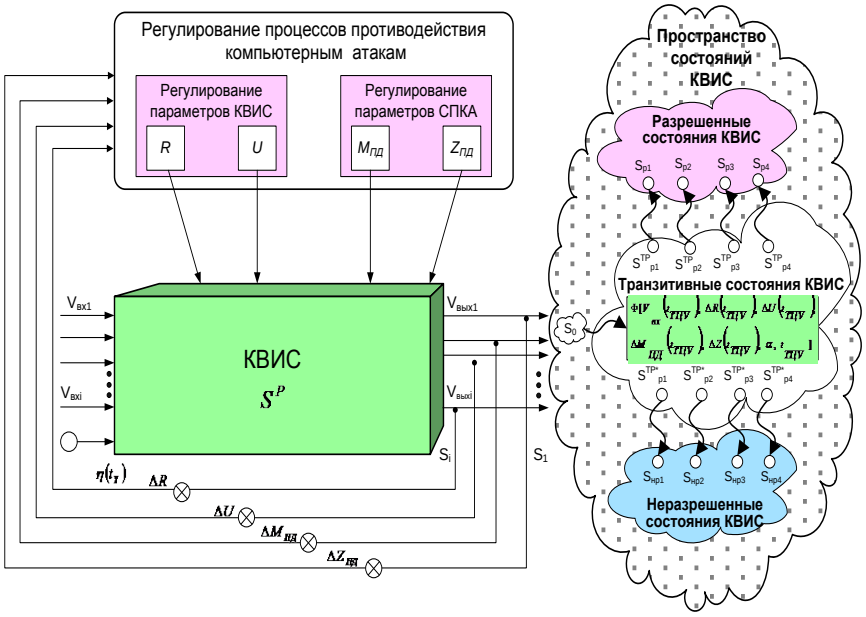

Рисунок 12 – Алгоритм динамических процессов регулирования КВИС

С этой целью на рисунке 12 пространство состояний процессов функционирования КВИС в условиях воздействия атак (S_T) идентифицируется в виде двух подпространств состояний: разрешенные состояния (множество компонент стабилизации состояний устойчивого функционирования КВИС) и неразрешенные состояния (множество состояний неустойчивого функционирования КВИС).

3. Идентификация пространства состояний КВИС на подпространства и области.

В частном случае, когда пространство состояний идентифицируется на подпространства и области, для каждой из которых задана непрерывная функция f и определены вектора регулирования уравнение (35) представляется в виде:

$$S^{P} = A(t_{ПДk})S + B(t_{ПДk})U + D(t_{ПДk})R + E(t_{ПДk})M_{ПД} + K(t_{ПДk})Z_{ПД} + \eta(t_{ok}), \qquad (37)$$

где A – матрица коэффициентов функции изменения состояний S во времени $(t_{ПДk})$ $n \times n$;

B - матрица коэффициентов функции изменения управляющих воздействий U во времени $(t_{ПДk})$ $n \times m$;

D - матрица коэффициентов функции изменения динамически регулируемых параметров КВИС R во времени $(t_{ПДk})$ $n \times d$;

E - матрица коэффициентов функции регулирования используемых методов, моделей и алгоритмов противодействия атакам $M_{ПД}$ и средств администрирования КВИС во времени $(t_{ПДk})$ $n \times e$;

K - матрица коэффициентов функции регулирования применяемых СПКА $Z_{ПД}$ во времени $(t_{ПДk})$ $n \times n$.

4. Формализация четырех процессов регулирования параметров КВИС и СПКА в момент времени противодействия.

Совокупность четырех процессов регулирования параметров КВИС и СПКА в момент времени противодействия $t_{ПДR+1}$, направленных на достижение состояния устойчивости функционирования КВИС при воздействии атак имеет вид:

$$S_{ПДk-1}\begin{cases} S_0 = const - \text{начальное состояние КВИС,} \\ \text{где } S_{ПДk\text{-}1} - \text{состояние КВИС } вв_{ПДk-1} - \text{момент времени,} \\ S_{\Delta U,\Delta R}(t_{ПДk-1}) = S_{ПДk} + B(t_{ПДk-1})U + D(t_{ПДk-1})R \to \max - \\ \text{- регулирование КВИС ,} \\ S_{\Delta M_{ПД}\Delta Z_{ПД}}(t_{ПДk-1}) = E(t_{ПДk-1})M_{ПД} + K(t_{ПДk-1})Z_{ПД} \to \max - \\ - \text{регулирование СПКА по противодействию атакам,} \\ \eta(t_{Yk-1}) = \min - \text{сведение } к\text{минимуму возможностей} \\ \text{воздействия атак через уязвимости КВИС.} \end{cases} \qquad (38)$$

5. Определение динамического процесса функционирования КВИС в условиях воздействия компьютерных атак при выполнении ограничений ТЦУ.

Динамический процесс функционирования КВИС в условиях воздействия компьютерных атак имеет вид уравнения (39) при выполнении ограничений ТЦУ:

$$
\text{м}_{\text{огр}}:\begin{cases}
\overline{v_{вых}}\left(t_{ПДk}\right)=S_t,\Delta R=v_{вх}\left(t_{ПДk}\right)-v_{вых}\left(t_{ПДk}\right),\\
\Delta R-\text{условие штатного выполнения ТЦУ};\\
t_д\to\min,t_p\to\min,t_{АП}\le t_{ТР},t_{ПД}\le t_{кр};\\
M_{ПД}\to M_{ТР},Z_{ПД}\to Z_{ТР},\eta\left(t_{Yk}\right)\to\min;\\
K_{ri}=\left\{\forall r_g\in R\mid F\left(t_{ПДk}\right)=M\left[B\left(t_{ПДk}\right)U+D\left(t_{ПДk}\right)R\right]\ge 0\right\};\\
\Delta R=R_{зд}\left(t_{ПДk}\right)-R\left(t_{ПДk}\right);\\
\Delta U=U_{зд}\left(t_{ПДk}\right)-U\left(t_{ПДk}\right);\\
\Delta M_{ПД}=M_{ПДзд}\left(t_{ПДk}\right)-M_{ПД}\left(t_{ПДk}\right);\\
\Delta Z_{ПД}=Z_{ПДзд}\left(t_{ПДk}\right)-Z_{ПД}\left(t_{ПДk}\right);\\
\overline{v}_{вх}\in V_{вх},\overline{v}_{вых}\in V_{вых}
\end{cases}
\qquad (39)
$$

При описании ограничений ТЦУ в соотношениях (39) приняты обозначения:

$v_{вх}$ - вектор входных параметров;

$v_{вых}$ – вектор выходных параметров;

$t_{кр}$ – критическое время выполнения ТЦУ;

K_{ri} – критические параметры сбора, обработки, передачи информации;

r_g – динамически регулируемые параметры КВИС;

$R_{зд}\left(t_{ПДk}\right)$ – заданное регулирование вектора внутренних параметров информационно-вычислительных ресурсов КВИС;

$U_{зд}\left(t_{ПДk}\right)$ - заданный вектор управляющих воздействий по регулированию выходной информации;

$M_{ПДзд}$ - заданные параметры вектора регулирования СПКА и средств администрирования КВИС при предупреждении, обнаружении и анализе компьютерных атак;

$Z_{ПДзд}$ – заданное регулирование вектора параметров активного противодействия компьютерным атакам на КВИС.

Для регулирования динамических процессов противодействия компьютерным атакам важно достижение устойчивости функционирования КВИС, то есть переход его в подпространство разрешенных состояний $\left(S_p\right)$.

6. Идентификация перехода КВИС в транзитивное и разрешенное состояния в условиях компьютерных атак.

Математические соотношения идентификации перехода КВИС в транзитивное (переходное) состояние и далее в разрешенные или неразрешенные состояния (правая

часть рисунка 12) в результате воздействия компьютерных атак и осуществления процессов противодействия им представляются следующим образом:

$$S^{TP}:\begin{cases}\Phi_{oi}\left(v_{вхi}\right): R\left[t_0,t_i\right]\rightarrow R\left[t_{ТЦУi}\right],\ i=1,...N\\ \Phi_{oj}\left(v_{вхj}\right): U\left[t_0,t_j\right]\rightarrow U\left[t_{ТЦУj}\right],\ j=1,...N\\ \Phi_{om}\left(v_{вхm}\right): M_{ПД}\left[t_0,t_m\right]\rightarrow M_{ПД}\left[t_{ТЦУm}\right],\ m=1,...N\\ \Phi_{or}\left(v_{вхr}\right): Z_{ПД}\left[t_0,t_m\right]\rightarrow Z_{ПД}\left[t_{ТЦУr}\right],\ r=1,...N\\ S_0=\varnothing - \text{непустое множество начальных состояний}\\ S_t\subset S_t^n - \text{n - мерное евклидово пространство состояний}\end{cases} \quad (40)$$

$$S_p:\begin{cases}\Phi_{pi}\left(v_{вхi}\right): R\rightarrow K_R\in K_{Ri}\mid\forall S_{tp1}^{TP}\in S_{ti}^{TP}\exists S_{tp1}^{TP}\rightarrow S_{tp1};\\ K_{Ri}\geq K_{Rn} - \text{порог срабатывания перехода в разрешенное состояние при регулировании } \Delta R;\\ \Phi_{pj}\left(v_{вхi}\right): U\rightarrow K_U\in K_{Uj}\mid\forall S_{tp2}^{TP}\in S_{tj}^{TP}\exists S_{tp2}^{TP}\rightarrow S_{tp2};\\ K_{Ui}\geq K_{Un} - \text{порог срабатывания перехода в разрешенное состояние при регулировании } \Delta U;\\ \Phi_{pm}\left(v_{вхi}\right): M_{ПД}\rightarrow K_{M_{ПД}}\in K_{M_{ПД\,m}}\mid\forall S_{tp3}^{TP}\in S_{tm}^{TP}\exists S_{tp3}^{TP}\rightarrow S_{tp3};\\ K_{M_{ПД\,m}}\geq K_{M_{ПД\,n}} - \text{порог срабатывания перехода в разрешенное состояние при регулировании } \Delta M_{ПД};\\ \Phi_{pr}\left(v_{вхi}\right): Z_{ПД}\rightarrow K_{Z_{ПД}}\in K_{M_{ПД\,r}}\mid\forall S_{tp4}^{TP}\in S_{tr}^{TP}\exists S_{tp4}^{TP}\rightarrow S_{tp4};\\ K_{Z_{ПД\,r}}\geq K_{Z_{ПД\,n}} - \text{порог срабатывания перехода в разрешенное состояние при регулировании } \Delta Z_{ПД}.\end{cases} \quad (41)$$

7. Идентификация перехода КВИС в неразрешенное состояние в результате воздействия компьютерных атак:

$$S_{нр}:\begin{cases}\Phi_{нрi}(v_{вхi}): R \to K^{*}{}_{R} \in K_{Ri} \mid \forall S_{tнр1}^{TP*} \in S_{ti}^{TP} \exists S_{tнр1}^{TP*} \to S_{tнр1};\\ K_{Ri}^{*} \geq K^{*}{}_{Rn} \text{ - порог срабатывания перехода в неразрешенное состояние при регулировании } \Delta R;\\ \Phi_{нрj}(v_{вхi}): U \to K^{*}{}_{U} \in K_{Uj} \mid \forall S_{tнр2}^{TP*} \in S_{tj}^{TP} \exists S_{tнр2}^{TP*} \to S_{tнр2};\\ K^{*}{}_{Ui} \geq K^{*}{}_{Un} \text{ - порог срабатывания перехода в неразрешенное состояние при регулировании } \Delta U;\\ \Phi_{нрm}(v_{вхi}): M_{ПД} \to K^{*}{}_{M_{ПД}} \in K^{*}{}_{M_{ПД\,m}} \mid \forall S_{tнр3}^{TP*} \in S_{tm}^{TP} \exists S_{tнр3}^{TP*} \to S_{tнр3};\\ K^{*}{}_{M_{ПД\,m}} \geq K^{*}{}_{M_{ПД\,n}} \text{ - порог срабатывания перехода в неразрешенное состояние при регулировании } \Delta M_{ПД};\\ \Phi_{нрr}(v_{вхi}): Z_{ПД} \to K^{*}{}_{Z_{ПД}} \in K^{*}{}_{Z_{ПД\,r}} \mid \forall S_{tнр4}^{TP*} \in S_{tr}^{TP} \exists S_{tнр4}^{TP*} \to S_{tнр4};\\ K^{*}{}_{Z_{ПД\,r}} \geq K^{*}{}_{Z_{ПД\,n}} \text{ - порог срабатывания перехода в неразрешенное состояние при регулировании } \Delta Z_{ПД}.\end{cases} \quad (42)$$

где «*» - означает неразрешенное состояние.

Соотношения (35 – 42) отражают условия динамических процессов функционирования КВИС в условиях воздействия атак, при которых система переходит в транзитивное состояние, а в результате регулирования параметров КВИС $(\Delta R, \Delta U)$ и СПКА $(\Delta M_{ПД}, \Delta Z_{ПД})$ может перейти в разрешенное или неразрешенное состояние при различных значениях динамически регулируемых параметров:

K_{Ri} – регулирование параметров информационно-управляющих ресурсов;

K_{Uj} - регулирование параметров управляющей информации по выполнению ТЦУ;

$K_{МПД\,m}$ - регулирование параметров СПКА и средств администрирования безопасности информации КВИС;

$K_{Z\,ППД}$ – регулирование параметров активного противодействия компьютерным атакам на КВИС.

Таким образом, модель динамических процессов противодействия компьютерным атакам для идентификации состояния КВИС основана на представлении процессов противодействия атакам математическими соотношениями с использованием параметров регулирования КВИС $(\Delta R, \Delta U)$, параметров регулирования используемых методов, моделей, алгоритмов и применяемых компонентов СПКА $(\Delta M_{ПД}, \Delta Z_{ПД})$, а также параметров перехода из транзитивных состояний S^{TP} в разрешенные состояния S_p устойчивого функционирования КВИС. Модель позволяет формализовать процессы

компенсации воздействий атак средствами СПКА при поступлении входной информации (выдачи выходной информации), корректировки информационно-вычислительного процесса, выработки управляющих выходных воздействий и восстановления информации КВИС.

Идентификация состояния КВИС на основе модели динамических процессов противодействия компьютерным атакам состоит в том, что предложены параметры регулирования средств противодействия атакам и идентификации состояния КВИС с целью обеспечения устойчивости ее функционирования в условиях воздействия компьютерных атак.

7 Показатели оценки противодействия компьютерным атакам на КВИС

Отечественные и зарубежные нормативно-технические документы по информационной безопасности КВИС на качественную оценку уровня защищенности, прежде всего средств вычислительной техники и автоматизированных систем (АС) в целом [15-24, 26, 27]. Эти документы включают в свой состав лишь отдельные требования к показателям программного и информационного обеспечения и не учитывают специфику функционирования сложных аппаратно-программных комплексов, объединенных распределенной вычислительной сетью, в условиях компьютерных атак. Один из первых подходов к комплексной и количественной оценке эффективности защиты информации компьютерных систем в динамике их функционирования рассмотрен в методах, приведенных в [69]. Стандарты, общие технические требования и руководящие документы, устанавливающие требования к системе показателей оценки противодействия компьютерным атакам на КВИС, находятся в стадии разработки.

В разделе представлены показатели оценки противодействия компьютерным атакам на КВИС, разработанные в интересах комплексного оценивания компьютерных атак нарушителя, оценки защищенности и устойчивости функционирования систем, средств противодействия атакам, и дополняющие документы по защищенности АС. Предлагаются следующие основные определения, используемые при разработке показателей.

Показатели оценки противодействия компьютерным атакам на КВИС должны позволять комплексно оценивать свойство устойчивости функционирования КВИС при воздействии компьютерных атак, опасность программно-аппаратных воздействий по нарушению (изменению) заданной технологии обработки информации и целенаправленному искажению информационно-вычислительного процесса, уязвимости КВИС и функциональные возможности средств противодействия.

Требования к разработке шкалы показателей противодействия определяются на основе анализа нормативных и руководящих документов, материалов по оценке защищенности КВИС при воздействии компьютерных атак [15-24, 26, 27, 29, 30, 44].

Ввиду наличия факторов неопределенности в реализации конкретного сценария атаки, состояния КВИС в периоды выполнения ТЦУ, в параметрах распознавания и ликвидации источника атак определять значения показателей средств противодействия

можно лишь вероятностным образом (шкала от 0 до 1) и экспертным путем (шкала весовых коэффициентов от 0 до 10).

На основе вероятностных характеристик можно образовать шкалу обобщенных показателей (качественных и количественных), а для анализа отдельных свойств средств противодействия атакам на КВИС использовать расчетные коэффициенты. Вероятностные характеристики позволяют оценить противодействие компьютерным атакам с учетом общецелевого применения КВИС и его программного обеспечения как основной системообразующей компоненты. Они используются как для интегральной оценки уровня устойчивости функционирования КВИС, так и для анализа отдельных свойств средств противодействия атакам. В интересах наиболее полной оценки противодействия компьютерным атакам шкала показателей включает в свой состав ряд коэффициентов и взаимосвязанных характеристик атак, КВИС и средств противодействия.

Структура шкалы показателей оценки противодействия компьютерным атакам на КВИС представлена в виде таблицы 2. При построении шкалы показателей используется принцип шкал соответствия. Вертикальными шкалами (столбцы таблицы) являются показатели оценки КВИС, компьютерных атак и средств противодействия атакам, прогнозируемые уровни устойчивости функционирования КВИС, типовые рубежи противодействия атакам и этапы оценки КВИС. Горизонтальными шкалами (строки таблицы) являются описания показателей оценки КВИС, компьютерных атак и средств противодействия атакам, прогнозируемые уровни устойчивости функционирования КВИС, типовые рубежи противодействия атакам и этапы оценки КВИС. Детализация показателей осуществляется в соответствии с таблицами 3-9.

С учетом анализа требований к шкале показателей оценки противодействия компьютерным атакам и факторов, влияющих на ее формирование, показатели делятся на следующие группы.

Таблица 2 – Шкала показателей оценки противодействия компьютерным атакам на КВИС

Показатели противодействия компьютерным атакам	Прогнозируемые уровни устойчивости функционирования КВИС	Типовые рубежи противодействия атакам	Этапы оценки КВИС и СПКА
I. Качественные показатели: 1. Оценка КВИС: – интегральная оценка весовых коэффициентов устойчивости функционирования КВИС; – проверка уязвимостей; – контроль восстанавливаемости; – соответствие функций ограничениям на выполнение ТЦУ; – способность к взаимодействию и согласованность работы внутренних компонентов КВИС и СПКА между собой и с внешними абонентами; – инвариантность и модифицируемость КВИС и СПКА при изменении входных и выходных данных и параметров атак; – наличие средств управления доступом к программам и данным; – наличие средств обеспечения целостности программ и данных. 2. Оценка СПКА: – полнота реализации функций; – наличие средств активного противодействия; – наличие датчиков СПКА в базовых компонентах КВИС. 3. Оценка нарушителя: – анализ возможных сценариев информационных акций – оценка предполагаемых способов, форм и средств реализации атак.	Высокий уровень устойчивости функционирования КВИС $P_{уф}$ = 0.9	1 – 7 рубежи	1. Обоснование требований. 2. Разработка (тестирование). 3. Предварительные испытания на стендовом полигоне. 4. Приемо-сдаточные испытания. 5. Ввод в эксплуатацию и сопровождение.
	Средний уровень устойчивости функционирования КВИС $P_{уф}$ = 0.7	1, 2 – рубежи не в полной мере, 3, 4 – рубежи, 5 – рубеж не в полной мере	Оценка отдельных средств на устойчивость функционирования в ходе испытаний на стендовом полигоне и при сдаче в эксплуатацию.
	Низкий уровень устойчивости функционирования КВИС $P_{уф}$ = 0.5	2, 3, 4 – рубежи не в полной мере	Устранение замечаний по результатам предварительных и приемо-сдаточных испытаний.

II. Количественные показатели: – показатели оценки уязвимости КВИС; – показатели оценки компьютерных атак на КВИС; – показатели оценки средств противодействия компьютерным атакам на КВИС; – показатели восстанавливаемости КВИС; – показатели оценки защищенности КВИС.			

1. Качественные и количественные показатели оценки устойчивости функционирования КВИС.

2. Количественные показателей оценки противодействия компьютерным атакам на КВИС, а именно:

- показатели оценки уязвимости КВИС;
- показатели оценки компьютерных атак на КВИС;
- показатели оценки средств противодействия компьютерным атакам на КВИС;
- показатели оценки восстанавливаемости КВИС;
- показатели оценки защищенности КВИС.

Качественные показатели оценки устойчивости функционирования КВИС используются для анализа влияния характеристик и вариантов построения системы и средств противодействия на устойчивость КВИС в целом, а также для прогнозирования его состояния при воздействии компьютерных атак.

На основе системного анализа нормативных документов и методик по оценке качества и устойчивости функционирования автоматизированных систем [4, 15-24, 26, 27, 29, 30, 44, 69] для оценки устойчивости функционирования КВИС выбран перечень показателей, представленный в таблице 3. При выполнении требований к качественному показателю КВИС его значение принимает «1», а при не выполнении «0».

Уровни устойчивости функционирования КВИС предназначены для ранжирования систем и включают в свой состав следующие уровни:

- высокий уровень, при котором производится оценивание и выполнение требований к устойчивости функционирования по совокупности

качественных и количественных показателей атак, средств противодействия, КВИС и результатам мониторинга системы на всех этапах жизненного цикла;

- средний уровень, при котором контроль устойчивости функционирования КВИС осуществляется не на всех возможных рубежах противодействия атакам, учитываются в полной мере только известные атаки, упрощается анализ и детализация характеристик применения КВИС (не учитываются качественные показатели);
- низкий уровень, при котором определяются лишь отдельные показатели оценки КВИС, угроз атак и средств противодействия им.

Показатели оценки уязвимости КВИС характеризуют полноту и достаточность принятых мер для предотвращения потенциальных угроз воздействия компьютерных атак и снижения риска потери устойчивости функционирования системы.

Таблица 3 – Показатели устойчивости функционирования КВИС

№ п/п	Обозначение показателя	Наименование показателя
Качественные показатели		
1.	$R_в$	Способность к взаимодействию с внешними абонентами КВИС.
2.	$R_с$	Согласованность работы между компонентами КВИС и СПКА.
3.	$R_о$	Выполнение временных и ресурсных ограничений ТЦУ.
4.	$R_и$	Инвариантность к изменяющимся потокам входных и выходных данных при реализации информационно-вычислительного процесса.
5.	$R_н$	Возможность гибкой настройки параметров КВИС и СПКА и их модифицируемость.
Количественные показатели		
6.	$P_{уф}$	Вероятность обеспечения устойчивости функционирования КВИС.
7.	$N_и$	Количество испытаний по оценке устойчивости функционирования КВИС.
8.	$\tau_н$	Нормализованное время, в течение которого производится оценка устойчивости функционирования КВИС.
9.	$T_{цi}$	Время одного испытательного цикла оценки устойчивости функционирования КВИС.
10.	$\tau_{от}$	Усредненное время оценки устойчивости функционирования КВИС.
11.	$T_м$	Время мониторинга устойчивости функционирования КВИС.

Оценка производится на основе анализа соответствия классификации компьютерных атак внедренным (планируемым к применению) методам и средствам противодействия компьютерным атакам на КВИС с использованием алгоритма противодействия компьютерным атакам на КВИС и определения показателей, представленных в таблице 4.

Таблица 4 – Показатели оценки уязвимости КВИС

№ п/п	Обозначение показателя	Наименование показателя
1.	M_y	Уязвимые места КВИС.
2.	$K_м$	Количество мер, принятых для противодействия угрозам воздействия компьютерных атак.
3.	K_y	Коэффициент уязвимости, равный отношению количества атак для которых приняты меры по их нейтрализации к общему количеству атак.
4.	$P_{цуяз}$	Вероятность использования уязвимостей КВИС при реализации атаки.

В качестве временных и вероятностных показателей оценки компьютерных атак на КВИС выбраны показатели, представленные в таблице 5.

В качестве показателей оценки средств противодействия компьютерным атакам на КВИС выбраны показатели, приведенные в таблице 6.

Таблица 5 – Показатели оценки компьютерных атак на КВИС

№ п/п	Обозначение показателя	Наименование показателя
1.	$P_{вд}$	Вероятность реализации воздействия компьютерных атак на КВИС.
2.	A_y	Количество компьютерных атак нарушителя.
3.	$T_д$	Время действия атак.
4.	M_y	Множество идентификационных параметров атаки.
5.	λ_y	Интенсивность атаки – среднее время между проявлением атаки.
6.	$Y_m = Y_c/Y_o$	Относительная полнота базы данных атак, где Yc – число атак, хранящихся в СПКА (сервере стендового полигона), Yo – общее число возможных угроз.
7.	Y_A	Потенциальные угрозы реализации атаки.
8.	J	Параметры нарушителя.
9.	B_Y	Средства реализации атаки.

10.	$P_{ск}$	Вероятность сканирования параметров КВИС.
11.	$P_{сбан}$	Вероятность проведения сбора и анализа характеристик КВИС.
12.	$P_{внрас}$	Вероятность внедрения и распространения компьютерных атак в КВИС.
13.	$P_{прп}$	Вероятность преодоления рубежей противодействия СПКА.

Таблица 6 – Показатели оценки средств противодействия компьютерным атакам на КВИС

№ п/п	Обозначение показателя	Наименование показателя
1.	$T_{пр}$	Время наступления события предупреждения атак.
2.	$T_{ан}$	Время анализа атак.
3.	$T_{об}$	Время обнаружения атак.
4.	$T_{ап}$	Время активного противодействия атакам.
5.	$m_{пд}$	Математическое ожидание продолжительности этапов противодействия.
6.	$\sigma_{эпд}$	Среднеквадратическая ошибка в определении времени этапа противодействия.
7.	$P_{п}$	Вероятность предупреждения воздействия атак.
8.	$P_{о}$	Вероятность обнаружения попыток реализации атак на КВИС.
9.	$P_{а}$	Вероятность анализа известных и неизвестных атак.
10.	$P_{поа}$	Вероятность предупреждения, обнаружения и анализа атак.
11.	$P_{уп}$	Вероятность успешного противодействия атакам.
12.	$P_{сб\ ап}$	Вероятность активного противодействия атакам.
13.	$P_{ла}$	Вероятность локализации атак в КВИС.
14.	$P_{лв}$	Вероятность ликвидации последствий внедрения атак.
15.	$P_{лр}$	Вероятность ликвидации последствий распространения атак в КВИС.
16.	$P_{лв}$	Вероятность ликвидации последствий воздействия атак.
17.	$P_{тр}$	Требуемое значение вероятности.
18.	$T_{дост}$	Время, при котором достигается требуемый уровень вероятности.

Оценка средств противодействия компьютерным атакам осуществляется во взаимосвязи с оценкой показателей информационно-вычислительного процесса КВИС и средств реализации компьютерных атак.

В качестве показателей оценки восстанавливаемости КВИС при воздействии на него компьютерных атак выбраны показатели, приведенные в таблице 7.

Таблица 7 – Показатели оценки восстанавливаемости КВИС

№ п/п	Обозначение показателя	Наименование показателя
1.	$P_в$	Вероятность восстановления КВИС после воздействия атак.
2.	$T_{св}$	Среднее время восстановления КВИС после воздействия атак.
3.	$S_в$	Наличие (отсутствие) средств автоматического (автоматизированного) восстановления работоспособности КВИС.

В качестве показателей оценки защищенности КВИС выбраны показатели, представленные в таблице 8.

Таблица 8 – Показатели оценки защищенности КВИС

№ п/п	Обозначение показателя	Наименование показателя
1.	$K_{фз}$	Количество реализованных функций защиты из следующего перечня: - проведение аудита, регистрации и учет событий; - обеспечение конфиденциальности информации для различных субъектов доступа; - обеспечение целостности данных, защита информации от искажения, модификации и уничтожения; - обеспечение контроля и управления доступом к данным; - обеспечение идентификации и аутентификации операторов; - обеспечение защищенной передачи данных; - обеспечение надежности средств защиты информации; - обеспечения администрирования ресурсов КВИС и СПКА.
2.	$V_{фз}$	Полнота реализации функций защиты, определяемая как отношение числа реализованных функций защиты к их общему количеству.

Оценка уровня защищенности КВИС складывается из количества и полноты реализованных функций защиты.

При оценке предложенных показателей в качестве варьируемых параметров выбраны параметры, представленные в таблице 9.

При моделировании и оценке показателей средств противодействия компьютерным атакам приняты следующие ограничения и допущения:

1. Требуемое значение вероятности события, что атака на КВИС не будет реализована $P_{тр}$ =0,95.

2. Методическая погрешность моделирования и оценки показателей средств противодействия на уровне 10-15%.

3. Значения вероятностей меньше 0,5 при оценке показателей средств противодействия и в расчет не берутся, в связи с невозможностью удовлетворения заданным требованиям при использовании предложенных методов и моделей противодействия компьютерным атакам на КВИС.

4. Для определения требуемого количества и объема испытаний КВИС необходимо использовать реальные данные программ и методик испытаний КВИС.

Значения вероятностных показателей могут быть получены в результате проведения экспертных оценок, натурных экспериментов, математического, имитационного и натурного моделирования на стендовом полигоне.

Таблица 9 – Варьируемые параметры оценки противодействия компьютерным атакам

№ п/п	Обозначение параметра	Наименование параметра
1.	$N_э$	Число экспериментов по противодействию атакам.
2.	$T_{КОi}$	Тип коммуникационного оборудования.
3.	$W_{СПОi}$	Вариант структуры СПО.
4.	$W_{ОПОi}$	Вариант структуры ОПО.
5.	V_i	Тип протокола передачи данных.
6.	$U_{пдкс}$	Скорость передачи данных в канале связи.
7.	V_u	Объем передаваемой информации.
8.	$T_{ВА}$	Время информационно-логического взаимодействия абонентов КВИС.
9.	I	Характеристики информационного обеспечения.
10.	$F_{квис}$	Совокупность функций КВИС.
11.	$T_{тцу}$	Интервал времени выполнения ТЦУ.
12.	$M_{пдi}$	Методы противодействия.

Таким образом, разработаны показатели оценки противодействия компьютерным атакам на КВИС, которые позволяют провести комплексную и количественную оценку средств противодействия компьютерным атакам и уровня устойчивости функционирования КВИС, а также обеспечить выбор наиболее приемлемой технологии создания средств противодействия атакам.

8 Априорный метод противодействия компьютерным атакам в терминах расширенных сетей Петри

8.1 Формализация априорного метода противодействия компьютерным атакам в терминах расширенных сетей Петри

Априорный метод противодействия компьютерным атакам на КВИС предназначен для формализации процессов компенсации воздействий атак, реорганизации информационно-вычислительного процесса, корректировки регламентов выполнения расчетных программ, выработки управляющих воздействий и восстановления устойчивости функционирования КВИС.

В наибольшей степени достижению целей разработки достоверной и адекватной математической модели описания процессов противодействия компьютерным атакам в сравнении с другим математическим аппаратом отвечают характеристики сетей Петри [5, 39, 54, 59].

Графическое представление процессов работы КВИС совместно с процессами противодействия атакам с помощью элементов сетей Петри удобно для исследования и интерпретации, легко и просто преобразуется в моделирующие алгоритмы и программы натурного и имитационного моделирования. При априорной оценке характеристик КВИС их описание с помощью сетей Петри позволяет представить облик структуры системы, определить механизм воздействия атак, выделить группы информационных и управляющих потоков.

Применение сетей Петри для разработки моделей средств противодействия атакам рассмотрено в материалах конференции [32-34].

Для формализации информационно-вычислительного процесса в КВИС при воздействии компьютерных атак и последующих процедур его восстановления используем расширенную сеть Петри (РСП).

На основе анализа подходов к формальному представлению сети Петри [5, 39, 54, 59] и ее расширений предлагается априорный метод противодействия компьютерным атакам на КВИС в терминах РСП определить в виде набора типовых математических элементов:

$$S_{КВИС} =< (P,V),T,D,M,Q,Ip\ ,Y >, \qquad (43)$$

где $P = p_1, p_2,..., p_i$ – непустое конечное множество позиций, характеризующих штатный режим функционирования КВИС (обозначается ○);

$V = v_1, v_2,..., v_j$ – множество позиций восстановления, отражающих процедуры восстановления при воздействии компьютерных атак (графически представляется □);

$T = t_1, t_2,..., t_n$ – непустое конечное множество переходов, при этом в соответствии с расширенными сетями Петри каждому переходу t_i может быть поставлен в соответствие алгоритм его срабатывания $a\lg_i$ (выделяется жирной вертикальной чертой ⏐, при наличии алгоритма над переходом делается пометка $a\lg_i$);

D – непустое конечное множество дуг сети, причем $D = (D_1 \cup D_2), D_1 = (P \times T) \cup (V \times T)$ – непустое множество входных дуг, соединяющих позиции и переходы, $D_2 = (T \times P) \cup (T \times V)$ – непустое множество выходных дуг, ориентированных от переходов к позициям;

M – множество маркировок позиций сети Петри;

$F_p : (M_p : P \to N), F_v : (M_v : V \to N)$ - функции начальной маркировки позиций штатного функционирования и восстановления соответственно, $N = \{ 0,1,2,... \}$ – множество натуральных чисел (помечается точкой внутри позиции ⊙);

Q - множество вероятностей запусков переходов, отражающее вероятности нахождения КВИС в режиме штатного функционирования, в моменты воздействия компьютерных атак (срабатывания датчиков СПКА) или в процессе восстановления;

$I_p = i_{p1}, i_{p2},..., i_{pm}$ – множество приоритетов для дуг;

$Y = y_1, y_2,..., y_k$ – множество временных параметров компьютерных атак, определяющее время срабатывания перехода в соответствии с временными задержками на перемещение маркеров или другими условиями, моделирующими обнаружение компьютерных атак и реакцию КВИС на них.

При этом под позициями сети понимаются реальные процессы в системе (или факт их запуска), а переходы, с учетом временных расширений РСП, позволяют оценить временные характеристики процессов противодействия атакам.

Предложенный аппарат расширенных сетей Петри ориентирован на событийно-стохастический подход к обобщенному анализу воздействия атак на КВИС, который

заключается в представлении информационно-вычислительных процессов в виде событий (интерпретируются переходами РСП), сменяющихся состояний (набор множеств P,V,T,M) и стохастических процессов, формализованных набором множеств (Q, I_p, Y) и отражающих вероятностные условия перехода КВИС из одного состояния в другое.

Позиции расширенной сети Петри интерпретируются условиями необходимыми для осуществления того или иного процесса. В отличие от стандартного набора множеств сети Петри, в расширенной сети Петри введены множества позиций восстановления V, вероятностей запусков переходов Q, приоритетов для дуг Ip, параметров компьютерных атак Y, обеспечивающие формализацию процесса функционирования КВИС при воздействии компьютерных атак. Элементы расширенной сети Петри служат основой для моделирования процессов функционирования КВИС, условий возникновения компьютерных атак и процессов противодействия им.

Априорный метод противодействия компьютерным атакам в терминах РСП формализует процесс функционирования реального КВИС и событий противодействия компьютерным атакам в структурно-параметрическом виде: структура процессов функционирования КВИС в условиях воздействия компьютерных атак – моделью графов, а параметры КВИС, компьютерных атак и средств противодействия атакам – математическими терминами РСП.

Данный метод представляется в виде трех элементов:

1. Модели регулирования информационно-вычислительного процесса (ИВП) в терминах расширенных сетей Петри, отражающей в обобщенном виде угрозы воздействия атак, динамику регулирования процессов функционирования компонентов КВИС и средств противодействия атакам (рисунок 13).

2. Модели реализации компьютерных атак на КВИС в терминах расширенных сетей Петри, формализующей механизмы реализации компьютерной атаки на КВИС и порядок преодоления рубежей противодействия в соответствии с планом нарушителя (рисунок 14).

3. Модели противодействия компьютерным атакам на КВИС в терминах расширенных сетей Петри, представляющей собой типовой граф и математические соотношения для описания процессов предупреждения, обнаружения, анализа компьютерных атак и активного противодействия атакам (рисунок 16).

8.2 Модель регулирования информационно-вычислительного процесса в КВИС в терминах расширенных сетей Петри

В модели регулирования информационно-вычислительного процесса КВИС (рисунок 13) применение средств противодействия компьютерным атакам формализуется моделью, состоящей из процессов: регулирования настроек СПКА и средств администрирования безопасности информации, регулирования информационных и вычислительных ресурсов КВИС, регулирования управляющей информации.

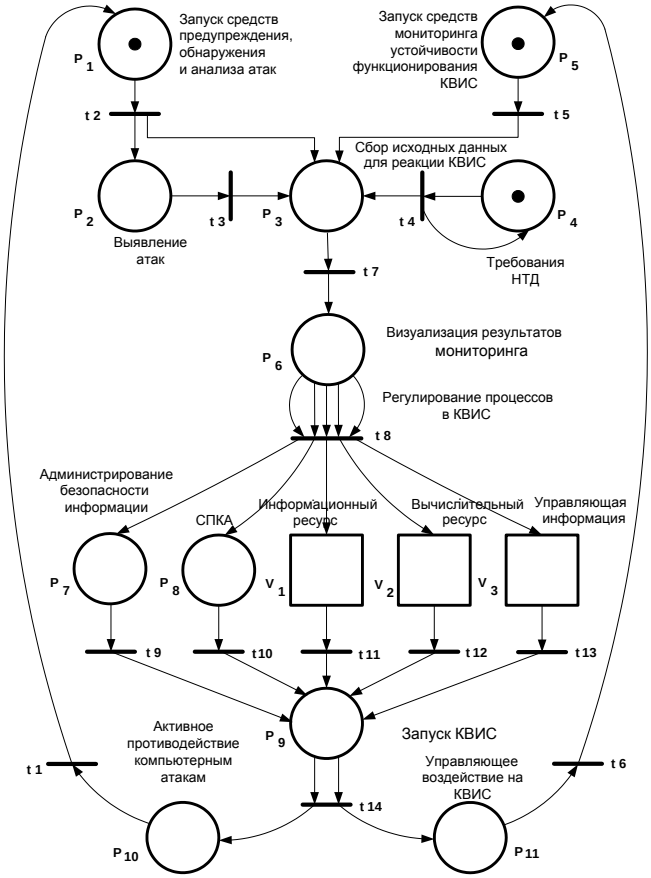

Рисунок 13 – Модель регулирования информационно-вычислительного процесса в КВИС в терминах расширенных сетей Петри

Модель регулирования процессов в КВИС при воздействии компьютерных атак отображает динамику перехода КВИС из одного состояния в другое вследствие регулирования ее параметров и обрабатываемых данных при выполнении ТЦУ и реагирования на компьютерные атаки. Анализ динамики работы модели регулирования информационно-вычислительного процесса, выполненной в терминах РСП, показывает,

что последовательность процессов запуска переходов соответствует режимам функционирования КВИС при воздействии атак. Динамика работы модели в терминах РСП осуществляется следующим образом (рисунок 13). Переход $t1$ и позиция $p1$ отображают запуск средств предупреждения, обнаружения и анализа атак и характеризуют начало процесса выявления воздействий атак (позиция $p2$ с соответствующим маркером, переход $t3$). Далее осуществляется запуск средств мониторинга устойчивости функционирования КВИС (позиция $p5$ с соответствующим маркером, переход $t5$).

Моделирование процесса сбора исходных данных для реакции КВИС и СПКА на атаки производится состоянием позиции $p3$.

Функции и параметры средств защиты информации от НСД определяются техническим заданием на КВИС, принятой классификацией атак и классами защищенности [27-29]: АС, средств вычислительной техники (СВТ), межсетевых экранов и антивирусных средств (позиция $p4$, переход $t4$).

Оперативное принятие решения по настройке средств администрирования СЗИ, выявления фактов воздействия атак и фильтрации пакетов данных принимается после наглядного отображения результатов мониторинга КВИС (позиция $p6$, переход $t7$).

Реакция КВИС на воздействие атак с вероятностью $q1$ отражается срабатыванием перехода $t8$ и соответствующих позиций $p7, p8,$ и позиций восстановления $v1, v2, v3$. Указанные позиции отражают прерывание информационно-вычислительного процесса в КВИС и корректировку параметров системы путем взаимосвязанной настройки средств СПКА и администрирования безопасности информации и программ, которые определяют характеристики информационного и вычислительного ресурсов и управляющих воздействий. Окончание восстановления информационно-вычислительного процесса в КВИС означает срабатывание переходов $(t9 - t13)$. После завершения регулирования ИВП и средств противодействия атакам производится рестарт программно-аппаратных средств КВИС и запуск ИВП с тех контрольных точек, с которых начинался процесс восстановления прерванного процесса функционирования КВИС (позиция $p9$).

Срабатыванием перехода $t14$ и нахождением КВИС в состояниях позиций $p10, p11$ имитируется решение двух задач, первой задачи, формирования управляющих воздействий на КВИС для нахождения соответствия между настройками КВИС и параметрами средств администрирования безопасности информации, и второй задачи, подготовки средств СПКА для противодействия потенциальным воздействиям атак.

Повторный цикл запуска средств предупреждения, обнаружения, анализа атак и мониторинга устойчивости функционирования КВИС с обновленными параметрами настройки моделируется срабатыванием переходов $t1, t6$ и позиций $p1, p5$.

Наличие начальной маркировки в позициях $p1, p5$ означает предпосылку, связанную с тем, что КВИС имеет возможность как статической, так и динамической настройки средств противодействия атакам при условии, если нарушение работы КВИС осуществляется программными средствами.

Модель регулирования ИВП, формализованная в терминах расширенной сети Петри, является типовой при априорном анализе воздействия атак на КВИС.

С учетом рассмотренной типовой модели регулирования ИВП в условиях противодействия атакам для метода моделирования компьютерных атак в терминах расширенных сетей Петри можно сформулировать правила срабатывания РСП, лежащие в основе динамики ее функционирования. Правила срабатывания РСП базируются на изменениях векторов маркировок сети M при запусках переходов t_n и ν_j. Для перемещения маркеров по РСП необходимо, чтобы выполнялись условия срабатывания переходов (так называемые предусловия) и были определены правила изменения маркировки позиции (постусловия) после запуска переходов. Поэтому правила срабатывания РСП включают: правило запуска перехода и правило изменения маркировки позиций при запуске переходов (кратко будет указываться – правило изменения маркировки).

Правило запуска перехода РСП.

Введем функции, позволяющие выразить структуру РСП в виде отображения множеств:

$$F_{d1} : P \times T \cup V \times T \to N, \text{ или иначе } F_{d1}(p_i, \nu_j, t_n),$$

$$F_{d2} : T \times P \cup T \times V \to N, \text{ или иначе } F_{d2}(t_n, p_i, \nu_j), \tag{44}$$

где F_{d1} – функция входных позиций, ставящая в соответствие позициям и переходам количество маркеров, необходимых для запуска перехода («входа»);

F_{d2} – функция выходных позиций, ставящая в соответствие позициям и переходам количество маркеров, необходимых для изменения маркировки (корректировки «выхода»);

$N = \{ 0,1,2,... \}$ – множество натуральных чисел.

Переход t_n может быть запущен, если в его входных позициях p_i и v_j находится не менее одного маркера, соответствующего каждой входной дуге, и нет маркеров в позициях, предшествующих запрещающим дугам. Используя кванторы общности и существования, это правило может быть представлено в следующем виде:

$$\forall(p_i \in P \wedge v_j \in V) \rightarrow \exists(M(p_1) \geq F_{d1}(p_i, v_j, t_n)) \quad (45)$$

Приведенное правило определяет условия осуществления конкретной стадии регулирования информационно-вычислительного процесса в КВИС.

Правило изменения маркировки РСП.

Если переход t_n сработал, то из каждой его входной позиции p_i и v_j удаляется количество маркеров $m(p_1)$ и $m(v_h)$, равное числу входных дуг, а в выходные позиции p_{i+1} и v_{j+1} добавляется число маркеров, равное числу выходных дуг. При этом происходит срабатывание перехода, которому соответствует наибольшее значение вероятности его запуска (q_w) и предшествует дуга с более высоким приоритетом (i_{pm}). Задержка на время срабатывания перехода определяется параметрами компьютерных атак (y_k) в позициях сети, из которых выходят дуги к этому переходу. По аналогии с записью предыдущего правила запишем:

$$\begin{aligned} &\forall(M_p \wedge M_v):(p_i \in P \wedge v_j \in V), \\ &\rightarrow \exists(M'_p \wedge M'_v) = F_p(Mp) + F_v(Mv) - F_{d1}(p_i, v_j, t_n) + F_{d2}(t_n, p_i, v_j). \end{aligned} \quad (46)$$

Функции F_{d1} и F_{d2} учитывают число входных и выходных дуг. На основе этого правила анализируются изменения начальной маркировки РСП при запуске того или иного перехода, т.е. прослеживаются стадии осуществления ИВП при воздействии атак на КВИС. В целом можно сказать, что правила срабатывания РСП позволяют представить динамику функционирования реального КВИС.

Таким образом, модель регулирования ИВП является элементом априорного метода противодействия компьютерным атакам в терминах расширенных сетей Петри и представляет собой структуру, выраженную в моделях элементов КВИС.

8.3 Модель реализации компьютерных атак на КВИС в терминах расширенных сетей Петри

Модель реализации процесса воздействия компьютерных атак на КВИС в терминах РСП (рисунок 14) в отличие от модели регулирования ИВП предназначена для детальной формализации процедур воздействия атак на КВИС путем реализации удаленного воздействия через сеть или на основе инициализации программной закладки (недекларированных возможностей в программах). Минимальный набор, необходимый для отображения процессов, связанных с реализацией атак на КВИС, выражается соотношением:

$$\exists \min(V, Q, D_z, I_p, Y) = S', \varphi : S' \to S^*. \tag{47}$$

Анализ последовательности элементов множеств из минимального набора S^* проводится на основе представления этих элементов следующими функциями:

$$\begin{aligned} \forall(v_j, q_w, d_{zc}, i_{pm}, y_k) \to \exists \psi_1 : \{\ 1,2,...j\ \} \to \{v_1, v_2, ...v_j\}, \\ \exists \psi_2 : \{\ 1,2,...w\ \} \to \{q_1, q_2, ...q_w\}, \\ \exists \psi_3 : \{\ 1,2,...n\ \} \to \{d_{z1}, d_{z2}, ...d_{zn}\}, \\ \exists \psi_4 : \{\ 1,2,...i\ \} \to \{i_{p1}, i_{p2}, ...i_{pm}\}, \\ \exists \psi_5 : \{\ 1,2,...k\ \} \to \{y_1, y_2, ...y_k\}. \end{aligned} \tag{48}$$

Введем L-множество индексов, тогда для каждого $l \in L$ существует S_l, которое есть подмножество множества S^*. Множество $\{\ (S'_l) l \in L\ \}$ является семейством подмножеств множества S^*. Функция $\psi : L \to S'$, значениями которой являются множества, представляет собой семейство множеств. Для этого семейства множеств можно записать соотношение $\psi(l) = S'_l$ и иначе обозначить его $(S'_l) l \in L$. Введение семейства множеств $(S'_l) l \in L$ позволяет определить функцию выбора через объединение семейства подмножеств в следующем виде:

$$\exists \psi : L \to \bigcup_L S'_l, \forall l (l \in L \to (l) \in S_l) \tag{49}$$

Графическим представлением расширенной сети Петри является ориентированный мультиграф с вершинами трех типов из множеств (P,V,T) и дугами из множеств D_1, D_2. Граф позволяет в статическом виде задать структуру КВИС.

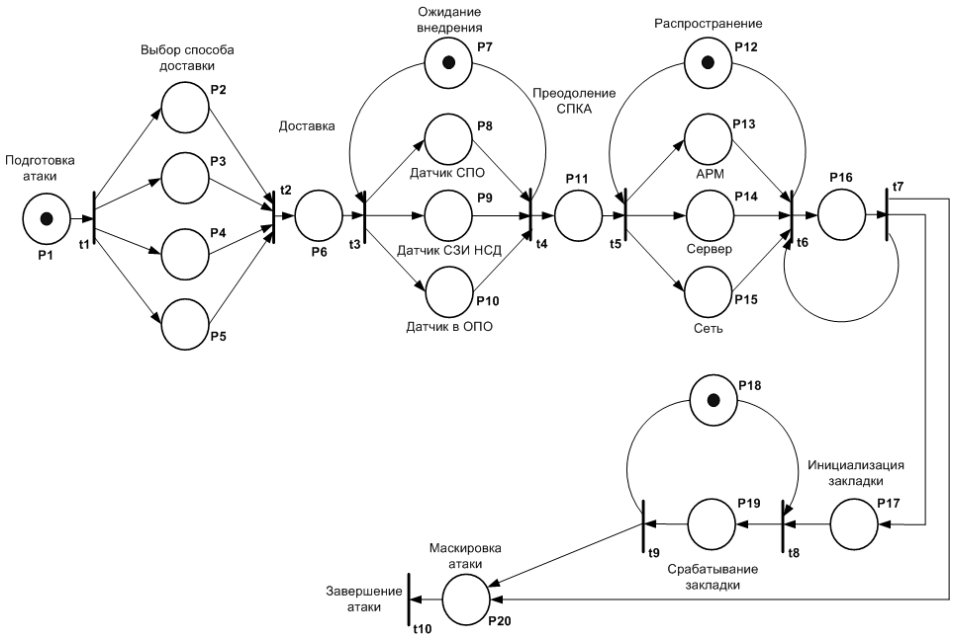

Рисунок 14 – Модель реализации компьютерных атак на КВИС в терминах расширенных сетей Петри

Моделирование динамики функционирования КВИС при воздействии компьютерных атак терминами РСП осуществляется путем введения маркеров в позиции (начальная маркировка) и перемещений их между позициями по правилам срабатывания переходов. Множество допустимых начальных маркировок задает, как и в обычных сетях Петри, начальное состояние расширенной сети Петри.

Маркировку РСП можно изображать двумя векторами M_p и M_v,:

$$M_p = \left(M(p_1), M(p_2), ..., M(p_i)\right); \quad M_v = \left(M(v_1), M(v_2), ..., M(v_j)\right), \tag{50}$$

у которых число компонент соответствует количеству «обычных» позиций и позиций восстановления, а значения i-х и j-х компонент равно количеству маркеров в позиции. Для задания достижимых маркировок (состояний) системы можно использовать диаграммы достижимых состояний.

Первоначальной стадией работы модели реализации компьютерных атак на КВИС в терминах РСП (рисунок 14) является подготовка исходных данных для начала компьютерной атаки, выбор или разработка атак специально для нарушения технологических циклов управления КВИС (позиция p1 с маркером).

Затем осуществляется выбор способа доставки атаки и выполнение самой доставки, что моделируется на схеме срабатыванием переходов t1, t2 и нахождением стадии выполнения атаки в позициях p2 – p6.

Возможными способами доставки атаки вероятнее всего будут передача данных через точки удаленного доступа распределенной вычислительной сети общего или специального назначения, по радиосети или через стандартные точки доступа ПЭВМ – беспроводная связь, а также путем использования уязвимостей или инициализации заблаговременно встроенных недекларированных возможностей.

Стадия реализации компьютерной атаки ожидание внедрения означает задержку на анализ СПКА и средств администрирования безопасности КВИС и подготовку к преодолению (взлому) конкретных рубежей противодействия в средствах противодействия компьютерным атакам, датчиков, встроенных в СПО и ОПО КВИС, СЗИ НСД и другие средства защиты информации (переход t3 и позиции p8 – p10). Наличие маркера в позиции p7 означает цикличность настройки функций взлома средств противодействия атакам для преодоления ограничений в СПКА на количество проверок полномочий субъекта или объекта доступа. Непосредственное преодоление СПКА представлено переходом t4 и позицией p11.

Распространение компьютерных атак в структуре КВИС и поражение информационного ресурса отдельных АРМ, серверов и протоколов передачи данных на различных уровнях эталонной модели взаимодействия открытых систем отражено переходом t5 и позициями p12 – p15. Реализация программного воздействия компьютерных атак зафиксирована срабатыванием перехода t6 и позицией p16.

Один из видов компьютерных атак, направленный на деструктивное воздействие на ИВП КВИС является применение программных закладок, описание типового цикла воздействия которых, моделируется переходами t 7, t 8 и позициями p17 – p19.

Скрытие фактов воздействия компьютерных атак на КВИС нарушителем осуществляется методами маскировки остаточной информации (бескомпроматности компьютерных атак), которые заключаются в удалении учетных записей в системных журналах, уничтожением программного кода атаки, уничтожением избыточных данных

(переходы t 7, t 9 и позиция p20). Полное завершение компьютерной атаки по нарушению информационных и вычислительных ресурсов КВИС фиксируется переходом t10.

Таким образом, модель реализации компьютерных атак на КВИС в терминах РСП, позволяет формализовать взаимосвязанные процессы: начала подготовки атаки, выбора способа доставки и ожидания внедрения атаки, преодоления рубежей СПКА и средств защиты информации, распространения атаки, инициализации и срабатывания программной закладки, маскировки и завершения атаки.

8.4 Модель противодействия компьютерным атакам на КВИС в терминах расширенных сетей Петри

Модель противодействия компьютерным атакам на КВИС в терминах расширенных сетей Петри базируется на модели динамических процессов противодействия компьютерным атакам. Эта модель объединяет в своем составе соотношения, формализующие процессы сбора, обработки, хранения, передачи и отображения информации в КВИС при выполнении ТЦУ, тип СПО, топологию сети передачи данных, возможные сценарии атак и реакцию средств противодействия на них. Стратегия моделирования процессов противодействия компьютерным атакам в терминах РСП осуществляется в соответствии с классификацией компьютерных атак.

Для математического описания в терминах расширенных сетей Петри комплексного решения проблемы противодействия компьютерным атакам на КВИС (жизненный цикл современных КВИС составляет приблизительно 15-20 лет) в общем случае необходимо (рисунок 15):

- определить настоящее устойчивое состояние функционирование КВИС $(P_{i+1}, n_{i+1}, e_{i+1}, b_{i+1})$ в условиях воздействия атак на основе данных о прошлом устойчивом состоянии КВИС (P_i, n_i, e_i, b_i) до воздействия атак (исходное состояние КВИС до воздействия атаки);
- спрогнозировать будущее устойчивое состояние КВИС $(P_{i+2}, n_{i+2}, e_{i+2}, b_{i+2})$ на основе имеющегося опыта противодействия компьютерным атакам (формализации паспортов новых атак в базе данных, регулирования параметров КВИС и СПКА).

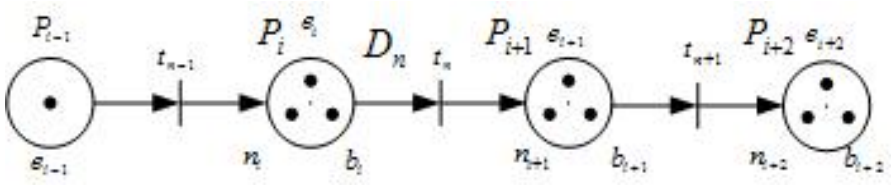

Рисунок 15 – Схема возможных состояний жизненного цикла КВИС в терминах расширенных сетей Петри

На рисунке 15 приняты следующие обозначения:

n_i - параметр, характеризующий настоящее устойчивое состояние КВИС на *i*-й момент времени;

e_i - параметр, описывающий прошлое устойчивое состояние КВИС на *i*-й момент времени;

b_i - параметр, представляющий будущее устойчивое состояние КВИС на *i*-й момент времени;

P_i - непустое конечное множество позиций (⊙);

t_n - непустое конечное множество переходов (|);

D_n - множество дуг сети (⟶);

$e_i \in E_{ki}$, $n_i \in N_{ki}$, $b_i \in B_{ki}$ - ограничение на РСП: нижний индекс «*к*» отражает, что существуют конечные множества значений параметров о прошлом, настоящем и будущем устойчивом состоянии КВИС.

Динамика работы расширенной сети Петри на рисунке 15 определяется $F_P : (M_P : P \to M)$ – функцией начальной маркировки (⊙). Маркировка из трех точек в позициях P_i, P_{i+1}, P_{i+2} означает, что для эффективного противодействия компьютерным атакам в *i*-й момент времени необходимо определить параметры настоящего, прошлого и будущего устойчивого состояния КВИС на основе моделирования динамических процессов функционирования системы.

Описание модели противодействия компьютерным атакам на КВИС в терминах расширенных сетей Петри представлено в виде базовой схемы анализа (рисунок 16): прошлого состояния КВИС (позиция P_{i+2} – задержка на обработку информации), настоящего состояния КВИС при воздействии атаки (позиция P_{n+4}) и будущего состояния КВИС – активного противодействия компьютерной атаке (переход t_{n+5}).

На основе использования базовой схемы модели противодействия компьютерным атакам на КВИС в терминах РСП, набора типовых математических элементов формулы (43) для реализации метода моделирования компьютерных атак в терминах РСП необходимо:

Шаг 1. Изобразить структуру КВИС со встроенными компонентами СПКА в виде графа событий (позиций РСП – P_i, V_i, $Z^*_{АПДi}$), условий возникновения событий (переходов РСП – T_i), вектора начальной маркировки (M_i), дуг и приоритетов дуг РСП (D_i и I_{pi}).

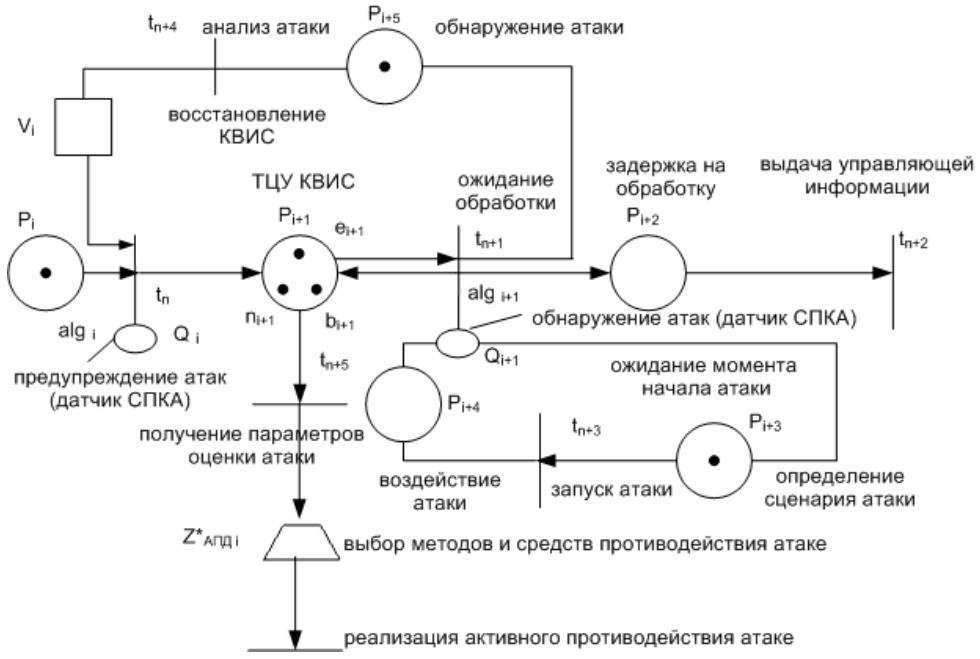

Рисунок 16 – Модель противодействия компьютерным атакам на КВИС в терминах расширенных сетей Петри

В составе графа РСП выделить основные фрагменты:

- имитации воздействия компьютерных атак;
- обнаружения и анализа компьютерных атак, восстановления информационно-вычислительного процесса КВИС;
- активного противодействия компьютерным атакам.

Шаг 2. Интерпретировать в виде математического описания состояния реальных процессов противодействия компьютерным атакам на КВИС в терминах расширенных сетей Петри с использованием конечных множеств значений параметров о прошлом, настоящем и будущем устойчивом состоянии КВИС ($E_{кі}$, $N_{кі}$, $B_{кі}$) в виде обобщенного функционала:

$$
\begin{aligned}
&S_{КВИСi} = F\left[(P_i, T_i, D_i, M_i, I_{pi}), Y_i, (V_i, Q_i, Z^*_{АПДi}), N_{ki}, E_{ki}, B_{ki}\right] \\
&F_{ud1}: P \times T \cup V \times T \cup Z^*_{АПДi} \times T \to N, \vee F_{ud1}(p_i, v_r, z_j, t_n), \\
&F_{ud2}: T \times P \cup T \times V \cup T \times Z^*_{АПДi} \to N, \vee F_{ud2}(t_n, p_i, v_r, z_j),
\end{aligned}
\tag{51}
$$

где F_{ud1} - функция инцидентности множеств входных позиций и переходов, ставящая в соответствие позициям и переходам количество маркеров, необходимых для запуска «входов» РСП;

F_{ud2} - функция инцидентности множеств выходных позиций и переходов, ставящая в соответствие позициям и переходам количество маркеров, необходимых для запуска «выходов» РСП;

$Z^*_{АПДi}$ – множество позиций активного противодействия компьютерным атакам (⏢);

и соотношения для взаимоувязанного применения КВИС и СПКА:

$$
S^{*ПД}_{КВИСi} = \sum_{i=1}^{m} S^*_{ki} \sum_{r=1}^{k} V_r \sum_{j=1}^{n} Z^*_{АПД\,j} \to \max, \tag{52}
$$

Если $Y_i = Y_{ki} \to \min$ (на этапе жизненного цикла КВИС при условии систематического устранения уязвимостей КВИС и ошибок в программном обеспечении), Y_{ki} – конечное множество атак, то

$$
\begin{aligned}
&Q_i \in Q_{ki} = \{q_1, q_2, ..., q_m\}, \\
&Q_{ki}: P_i \times V_i \times T_i \to \{1,0\} \to N,
\end{aligned}
\tag{53}
$$

где Q_{ki} - конечное множество срабатываний датчиков при выполнении функции инцидентности множеств позиций и переходов;

N - натуральный ряд чисел, образуемый суммированием единиц (зафиксированными событиями срабатывания датчиков СПКА).

Шаг 3. Описать начальную маркировку (M_i) в РСП для отображения и анализа причинно-следственных связей между процессами в КВИС и СПКА при воздействии атак

и условия оценки достижимости РСП (возможности перемещения маркеров по графу без попадания в тупиковую ситуацию):

$$F_p : (M_p : P \to N), F_V : (M_V : V \to N), F_Z : (M_Z : Z^*_{АПД} \to \mathrm{N}) \quad (54)$$

Тогда изменение маркировки $M'(p_i, v_r, z_j)$ на произвольный момент времени определяется из соотношения:

$$\begin{aligned} &\forall (p_i \in P \wedge V_r \in V \wedge Z_j \in Z^*_{АПД}) \to \\ &\exists M'(p_i, v_r, z_j) = M(p_i, v_r, z_j) - \left[F_p(M_p) + F_v(M_v) + F_z(M_z)\right] - \\ &\left[F_{ud1}(p_i, v_r, z_j, t_n) + F_{ud2}(t_n, p_i, v_r, z_j,)\right], \end{aligned} \quad (55)$$

причем

$$\forall m_i \in M_i \exists \min\{M_p, M_v, M_z\}, M_i = M_p \cup M_v \cup M_z.$$

Формула (55) является условием оценки достижимости РСП.

Шаг 4. Определить логические условия для срабатывания переходов РСП (T_i) при маркировке $M(p_i, v_r, z_j)$:

$$\begin{aligned} &\forall (p_i \in P \wedge V_r \in V \wedge Z_j \in Z^*_{АПД}) \to \\ &\exists \left[M(p_{i1}, v_{r1}, z_{j1}) \geq F_{ud1}(p_i, v_r, z_j, t_n)\right], \\ &\Psi_t \left[(p_{i1}, v_{r1}, z_{j1}), \ldots, (p_{in}, v_{rn}, z_{jn})\right] = 1, \end{aligned} \quad (56)$$

где Ψ_t - функция распределения маркировки по входным позициям РСП.

Шаг 5. Определить соотношения для позиций РСП, при условии синхронизации переходов (T_i)на i-м моменте времени противодействия компьютерным атакам с реальными событиями в КВИС через промежуточные состояния («подсобытия» P_i, V_i, $Z^*_{АПДi}$ предупреждения, обнаружения, анализа компьютерных атак и активного противодействия им, восстановления КВИС):

$$\forall(p_i \in P, e_i \in E_{ki}, n_i \in N_{ki}, b_i \in B_{ki} \rightarrow$$
$$\exists \min(p_i, V_r, Z_j, E_{ki+1}, N_{ki+1}, B_{ki+1}) \rightarrow Z^*_{ПД} \rightarrow, \Psi_{тн} = \{(p_{i1}, V_{r1}, Z_{j1}), \ldots (p_{in}, V_{rn}, Z_{jn})\}, \quad (57)$$
$$\Psi_{тн}(p_i, V_r, Z_j) = \begin{cases} 1, \text{если } m_{pi} \in M_p, m_{vr} \in M_v, m_{zj} \in M_z, \\ \varnothing, \text{если } m_{pi} \notin M_p, m_{vr} \notin M_v, m_{zj} \notin M_z, \end{cases}$$

где $\Psi_{тн}$ - функция начального входного распределения маркеров по позициям РПС;

$\min(p_i, V_r, Z_j, E_{ki+1}, N_{ki+1}, B_{ki+1})$ - необходимый минимум позиций РПС и параметров устойчивости функционирования КВИС, при которых функция противодействия компьютерным атакам стремиться к максимуму.

Условие (57) определяет порядок начального размещения маркеров по позициям РСП.

Шаг 6. Задать условия срабатывания датчиков СПКА (Q_i):

$$\forall t_i \in T, Q_{ki} \in Q, \exists Q_{i+1} \neq 0,$$
$$\varphi_q(t_i, Q_{ki}) = \begin{cases} 1, \text{если } mp_i \in M_p, y_i \in Y, a\lg_i = 1, \\ 1/R, \text{если } mp_i \in M_p, y_i \notin Y, a\lg_i = 1, \\ \varnothing, \text{в противном случае, } al_i = 0, \end{cases} \quad (58)$$

где $a\lg_i$ – алгоритм срабатывания датчика.

Выражение (58) определяет условия срабатывания датчика СПКА следующим образом:

$\varphi_q(t_i, Q_{ki}) = 1$ - датчик сработал, атака обнаружена;

$\varphi_q(t_i, Q_{ki}) = 1/R$ - ложное срабатывание датчика при R-м срабатывании перехода;

$\varphi_q(t_i, Q_{ki}) = \varnothing$ - датчик не сработал, неизвестная атака не обнаружена.

При выполнении последовательности реализации метода с 1-го шага по 6-й шаг определяются состояния процессов противодействия компьютерным атакам, происходящие в КВИС в настоящем, состояния, предшествовавшие этим процессам и состояния, в которые перейдет система после выполнения противодействия атакам. Разработка событийной модели реализации процесса компьютерных атак на КВИС в терминах РСП включает описание работы системы и проведение анализа процедур срабатывания переходов согласно маркировке сети, по результатам которого делается вывод о том, в каких состояниях находилась система и какие состояния не достижимы.

На рисунках 17 и 18 приведены примеры применения априорного метода противодействия компьютерным атакам в терминах расширенных сетей Петри для разработки моделей противодействия известным компьютерным атакам и устойчивости функционирования КВИС при воздействии известных и неизвестных компьютерных атак соответственно.

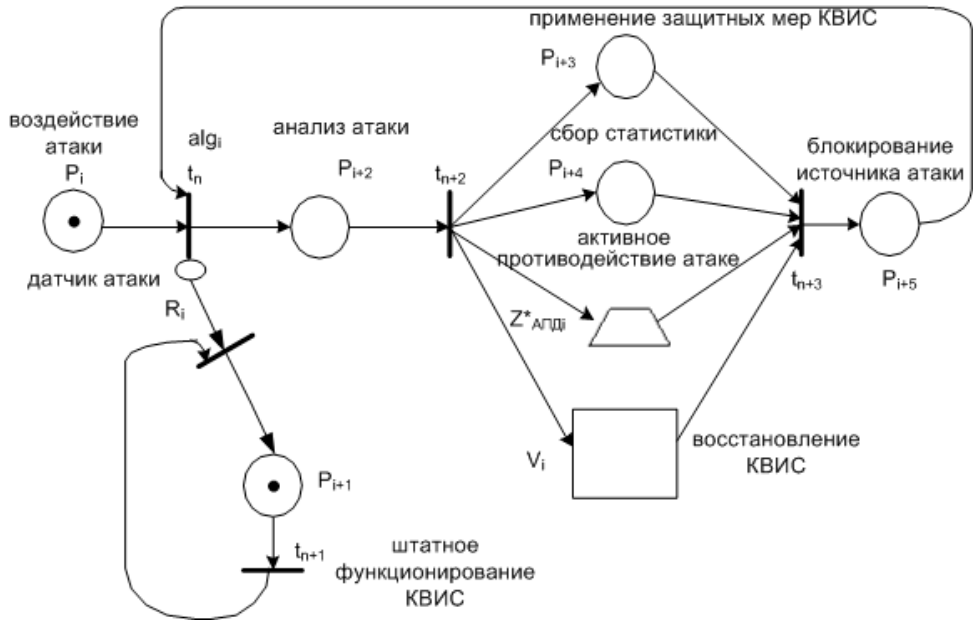

Рисунок 17 – Модель противодействия известным компьютерным атакам

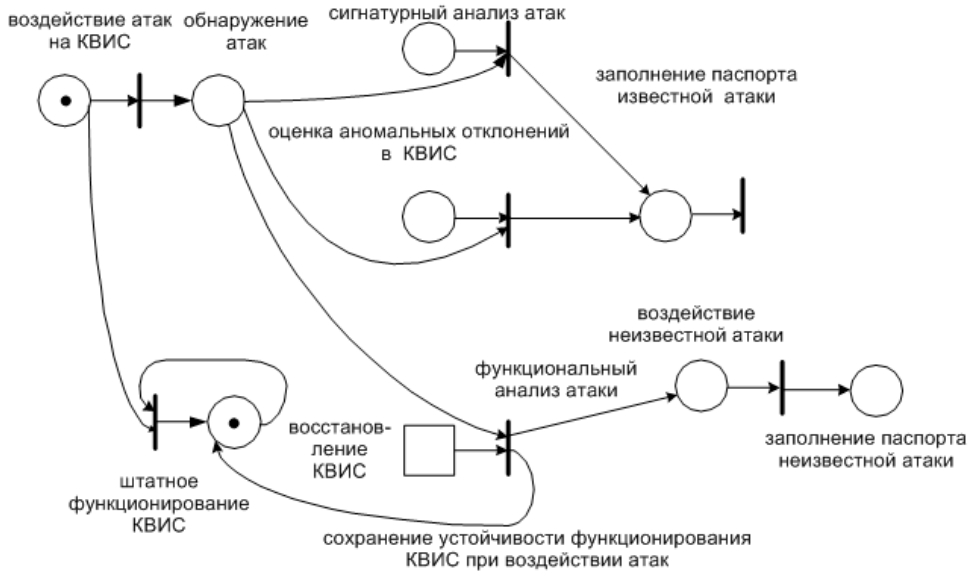

Рисунок 18 – Модель устойчивости функционирования КВИС при воздействии известных и неизвестных компьютерных атак

В целом на основании анализа приведенной совокупности математических моделей, априорный метод противодействия компьютерным атакам в терминах расширенных сетей Петри характеризуется следующим образом:

- является простым и удобным средством моделирования информационно-вычислительных процессов в КВИС, реализации компьютерных атак на КВИС и работы его программных компонентов в условиях противодействия атакам;
- обеспечивает выработку предложений по совершенствованию средств администрирования безопасности информации КВИС и доработке функций динамического восстановления информационно-вычислительного процесса КВИС и функций по противодействию компьютерным атакам;
- облегчает моделирование информационно-вычислительного процесса в КВИС во взаимосвязи с процессами устойчивости функционирования и активного противодействия компьютерным атакам;
- предоставляет минимальный набор средств для отображения процессов, связанных с противодействием атакам на КВИС, выражаемый элементами $\exists \min\{P_i, V_i, Z^*_{АПДi}, T_i, M_i, Q_i, D_n\}$.

9 Метод предупреждения компьютерных атак на критически важные информационные системы

Метод предназначен для мониторинга угроз подготовки компьютерных атак на КВИС и предотвращения возможностей (устранения условий) для их реализации. Он основан на контроле выполнения состояний выполнения ТЦУ при функционировании компонентов КВИС, оценке уязвимостей и определении фактов подготовки атак нарушителем (мониторинг опасности воздействия компьютерных атак) путем нахождения функции предупреждения на заданном интервале времени [36].

Исходными данными метода являются:

– параметры контроля состояния выполнения ТЦУ в КВИС:

S_i, X_i – состояния и события выполнения ТЦУ в КВИС соответственно;

$t_{ТЦУ_i}$ – время выполнения регламентов ТЦУ;

$V_{итрi}, T_{трi}$ – технологические ограничения на объем и периоды времени поступления и выдачи информации соответственно;

$K_э^{уст} = \{ к_{э1},..., к_{эi} \}$ – параметры эталонного состояния устойчивости функционирования системы, (состояние полученных данных, протоколов передачи данных, времени получения информации и выдачи управляющих воздействий и других параметров);

$K_{конт} = \{ к_{конт1},..., к_{контi} \}$ – параметры контроля реального состояния КВИС (фактические критически важные процессы функционирования КВИС при выполнении ТЦУ);

– параметры мониторинга опасности воздействия компьютерных атак:

$t_{мон_i}$ – время мониторинга устойчивости функционирования КВИС;

$\xi_{УЯЗП}$ – потенциальные уязвимые места КВИС;

$Y_{АП}$ – потенциальные угрозы реализации атаки;

$J_{kП}$ – потенциальные сценарии компьютерных атак нарушителя (на основе характеристик известных прототипов сценариев для подобных КВИС; например, информационно-телекоммуникационных средств на базе протоколов TCP/IP).

Алгоритм предупреждения компьютерных атак на КВИС приведен на рисунке 19.

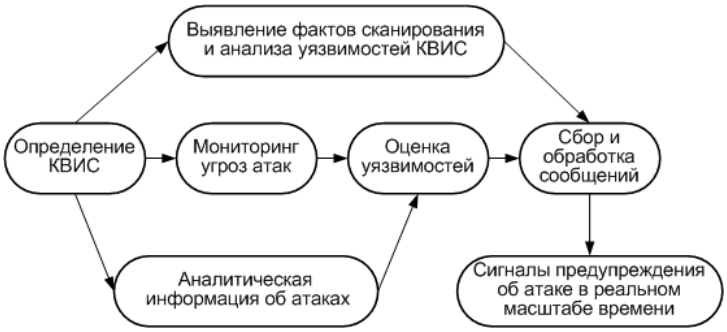

Рисунок 19 – Алгоритм предупреждения компьютерных атак на КВИС

Последовательность реализации метода предупреждения компьютерных атак на КВИС состоит в осуществлении следующих действий:

1. Определить структуру и параметры оцениваемого КВИС (построить имитационную модель КВИС).
2. Провести работу по анализу сценариев компьютерных атак нарушителя.
3. Провести мониторинг угроз атак и оценку уязвимостей реального КВИС (если имеется возможность, если нет, то провести имитационное моделирование компьютерных атак на КВИС на стендовом полигоне).
4. По данным, полученным в результате сбора и обработки сообщений от реального КВИС или имитационного моделирования его прототипа, предполагаемым аналитическим данным за время $t_{мон_i}$ определить $\xi_{УЗВП}$, Y_A, J_{uk}, $K_{мониi}$.
5. Проверить отличия параметров контроля состояния выполнения ТЦУ в КВИС (модели КВИС) и мониторинга опасности воздействия компьютерных атак от допустимого (заданного) значения, выдать сигналы предупреждения об атаке в реальном масштабе времени (извещение – «признаки подготовки компьютерной атаки») средствам обнаружения компьютерных атак.
6. Уточнить параметры эталонного устойчивого состояния системы $K_э^{уст}$.
7. Продолжить следующий цикл реализации мониторинга состояния КВИС.

Математические соотношения метода предупреждения компьютерных в определении двух функций предупреждения: по мере отличия параметров реального состояния КВИС от эталонного состояния и на основе мониторинга уязвимостей КВИС и признаков компьютерных атак:

1. Функции предупреждения компьютерных атак, основанной на выявлении отличия параметров реального состояния КВИС от его эталонного состояния:

$$G_{пр}^{кон}(t_{ТЦУ} \le t_{зад}^{'}):\begin{cases}\forall t_{ТЦУi} \in T_{ТЦУ}, S_i \in S, X_i \in X, \varphi(N_k) \ge \varphi(N_н^{уст}),\\ \exists\left[f_р(K_{контi} \in K_{конт}) - f_э(K_{эi} \in K_э^{уст})\right] \ge \alpha_{контi} \to \Delta_{кi} \in \Delta_{у,}\\ если\ (V_{и\ трi} < V_{и\ тр\ зад}) \vee (V_{и\ трi} > V_{и\ тр\ зад}) \ge \beta_{конт}, то\ \exists\Delta_{vi} \in \Delta_у,\\ если\ (T_{трi} < T_{тр\ зад}) \vee (T_{трi} > T_{тр\ зад}) \ge \gamma_{конт}, то\ \exists\Delta_{ti} \in \Delta_у,\end{cases} \quad (59)$$

где $G_{пр}^{кон}(t_{ТЦУ} \le t_{зад}^{'})$ – функция предупреждения компьютерных атак за счет контроля устойчивости функционирования КВИС;

$t_{зад}^{'}$ – заданное время контроля устойчивости функционирования КВИС;

N_k – количество контрольных наблюдений за состоянием КВИС;

$N_н^{уст}$ – количество фактов нарушения устойчивости функционирования КВИС;

$\alpha_{контi}$ – проверочные значения параметров $K_{контi}$;

$\Delta_{кi}$ – множество выявленных фактов отклонения критически важных регламентов сбора, хранения, обработки и передачи информации от заданных;

$\Delta_у$ – множество признаков компьютерных атак, выявленных на этапе их предупреждения;

$\beta_{конт}$ – проверочные значения параметров $V_{и\ трi}$;

Δ_{vi} – множество выявленных фактов отклонения $V_{и\ трi}$ от заданных значений $V_{и\ тр\ зад}$;

$\gamma_{конт}$ – проверочные значения параметров $T_{трi}$;

Δ_{ti} – множество выявленных фактов отклонения $T_{трi}$ от заданных значений $T_{тр\ зад}$.

2. Функции предупреждения компьютерных атак на основе мониторинга уязвимостей КВИС и признаков компьютерных атак:

$$G_{пр}^{мон}(t_{мон} \le t_{зад}^{''}):\begin{cases}\forall \varphi(N_k) \ge \varphi(N_{ck}), \varphi(N_k) \ge \varphi(N_{ан}),\\ \exists f_р(\xi_{уяз\ Фi} \in \xi_{уяз\ Ф}) - f_э(\xi_{уяз\ Пi} \in \xi_{уяз\ П}) \ge \alpha_{мониi} \to \Delta_{\xi} \in \Delta_у,\\ \exists f_р(\mathrm{Y}_{АФi} \in \mathrm{Y}_{АФ}) - f_э(\mathrm{Y}_{АПi} \in \mathrm{Y}_{АП}) \ge \beta_{мониi} \to \Delta_{уАФ} \in \Delta_у,\\ \exists f_р(I_{КФi} \in I_{КФ}) - f_э(I_{КПi} \in I_{КП}) \ge \gamma_{мон} \to \Delta_{Ii} \in \Delta_у,\end{cases} \quad (60)$$

где $G_{пр}^{мон}(t_{мон} \le t''_{зад})$ – функция предупреждения компьютерных атак, которая позволяет выявлять признаки атак за счет мониторинга опасности воздействия компьютерных атак;

$t''_{зад}$ – заданное время мониторинга опасности воздействия компьютерных атак;

$N_{ск}$ – количество фактов сканирования параметров КВИС;

$N_{ан}$ – количество фактов анализа уязвимостей КВИС;

$\xi_{уяз\,Фi}, \mathrm{Y}_{АФi}, I_{КФi}$ – фактические параметры уязвимостей КВИС, угроз воздействия атак и сценариев нарушителя соответственно;

$\alpha_{мониi}$ – проверочные значения параметров уязвимостей КВИС;

Δ_{ξ} – множество выявленных фактов наличия уязвимостей КВИС;

$\alpha_{мониi}$ – проверочные значения параметров наличия признаков компьютерных атак;

$\Delta_{уАФ}$ – множество выявленных признаков компьютерных атак;

$\gamma_{мон}$ – проверочные значения параметров реализации компьютерных атак;

Δ_{Ii} – множество выявленных фактов подготовки компьютерных атак нарушителем.

Выполнение условия предупреждения компьютерных атак при заданных исходных данных метода имеет вид:

$$G_{пр}(S_{КВИС}^{уст}) = \sum_{i=1}^{m}\sum_{k=1}^{n} S_i(t_{ПЦУi}) Y_{АК}^{OY}(t_{yk})$$
$$\left[G_{пр}^{кон}(t_{ПЦУ} \le t'_{зад}) + G_{пр}^{мон}(t_{мон} \le t''_{зад})\right] \to \max \qquad (61)$$

Эффект от применения метода предупреждения компьютерных атак на КВИС состоит в определении условий, которые должны гарантировать предотвращение компьютерных атак или обеспечить заблаговременную подготовку к их обнаружению и отражению на ранних стадиях нарушения выполнения ТЦУ в КВИС на основе мониторинга компьютерных атак.

10 Комбинированный метод обнаружения компьютерных атак на КВИС

Комбинированный метод обнаружения компьютерных атак на КВИС основан на определении совокупности функций обнаружения компьютерных атак – сигнатурного анализа, выявления аномалий и функционального анализа, проверяемых по комплексу условий расхождения с типовым ТЦУ сбора, обработки и передачи информации КВИС.

Исходные данные метода:

Y_{Ai} – множество атак нарушителя;

$T_{прг}$ – пороговое значение выполнения ТЦУ;

$V_{прг}$ – пороговое значение поступающей информации;

$f_{КВИС}^{ТЗ}$ – функции КВИС, установленные техническим заданием;

l_a – сигнатуры атак.

Алгоритм обнаружения компьютерных атак на КВ представлен на рисунке 20.

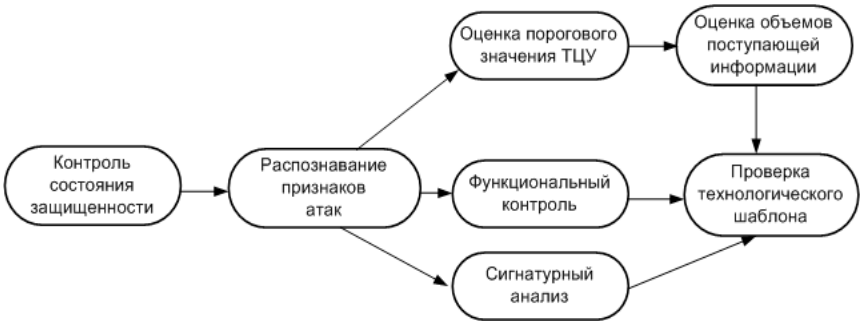

Рисунок 20 – Алгоритм обнаружения компьютерных атак на КВИС

Последовательность реализации комбинированного метода обнаружения компьютерных атак на КВИС:

1. Проанализировать результаты контроля защищенности КВИС.
2. Провести распознавание признаков компьютерных атак по параметрам датчиков путем поиска расхождений между технологическими шаблонами штатного выполнения ТЦУ и реальным процессом работы КВИС на основе:

– выявления аномалий по оценке пороговых значений ТЦУ (оценить время поступления входной информации, выдачи выходной информации и

внутреннего обмена данными в КВИС; оценить объемы поступающей информации);

– проведения функционального анализа КВИС и выявления нештатных функций;
– выявления признаков множества сигнатур компьютерных атак.

3. Выдать данные об обнаруженных компьютерных атаках в необходимом объеме для дальнейшего анализа и принятия решения по активному противодействию атакам путем определения функций обнаружения компьютерных атак:

а) обобщенной функции обнаружения компьютерных атак:

$$G_{об}(t_{ТЦУ} \le t_{зад}) = \sum_{i=1}^{R}(G_{обi}^{СГ} + G_{обi}^{АН} + G_{обi}^{ФА}) \to \max \qquad (62)$$

б) сигнатурного анализа компьютерных атак:

$$G_{обi}^{СГ}(t_{ТЦУ} \le t_{зад}): \begin{cases} \forall S_i \in S, X_i \in X, Y_i \in Y, A_i \in A, \\ \exists V_{вх} \ne V_{зад} \left| l_{ai} \subset Y_A, l_{ai} \in L_a = l_a^{б} \cap L_a^{ц}; \right. \\ \exists \left[(V_{итрi} = V_{ивх} \cup V_{ивых} \cup V_{ивн}) \ne V_{изад} \left| \bigcup_{i=1}^{k} l_{ai}(V_{итрi}) \in Y_A \right. \right] \ge \mu_{об}, \\ \Delta l_a \in \Delta_Y; \forall L_a \subset Y_A \left| l_a \le l_{зад}, \to \exists F_{об}^{СПКА}(l_{ai}) \le l_{зад} \to \max, \right. \end{cases} \qquad (63)$$

где $l_{ai} \in L_a$ – множество сигнатур компьютерных атак;

$L_a^{б}$ – множество последовательностей букв русского и английского алфавитов, входящих в сигнатуры атак;

$L_a^{ц}$ – множество арабских цифр, входящих в сигнатуры атак;

Δ_{la} – множество выявленных факторов сигнатур атак;

$F_{об}^{СПКА}(l_{ai})$ – функция обнаружения сигнатур компьютерных атак, реализованная в СПКА.

в) выявления аномалий при работе КВИС:

$$G_{обi}^{АН}(t_{ТЦУ} \le t_{зад}): \begin{cases} \forall t_{ТЦУi} \in T_{ТЦУ}, \xi_{УЯЗi} \in \xi_{УЯЗ}, Y_{Ai} \in Y_A, A_i \in A, \\ \exists\left[(V_{итр} \ge V_{прг}) \vee (t_{ТЦУi} \ge T_{прг})\right] S_j(T_{ТЦУ}) \notin S, \\ X_j(V_{итр}) \notin X, \rightarrow \Delta_{VT} \in \Delta_Y, \end{cases} \quad (64)$$

где Δ_{VT} – множество выявленных аномальных явлений по срабатыванию условия превышения пороговых значений выполнения ТЦУ и объемов поступающей информации КВИС.

г) функционального анализа КВИС:

$$G_{обi}^{ФА}(t_{ТЦУ} \le t_{зад}): \begin{cases} \forall f_{КВИС}: \mathrm{X} \rightarrow \mathrm{S}, \exists f_{КВИС} = \{f_{КВИС\,1}, ..., f_{КВИС\,j}\} - \\ \text{множество функций } КВИС, \quad \text{т о г д а} \\ \exists X_f = \{X_{f1}, ..., X_{f2}\} - \text{область изменения } f_{КВИС\,j}, \\ \text{соответствующая событиям } КВИС\text{-}X_i; \\ \exists \Gamma = \sum_{j=1}^{k} (f_{КВИС\,j} \wedge X_{fj}) \le \Gamma_{доп} - \text{условие проверки} \\ \text{технологического шаблона КВИС по ограничениям} \\ \text{на допустимые функции сегмента;} \\ \text{если } \exists f_{КВИС\,j} \in f_{КВИС}^{ТЗ} \left| \Gamma_j = (f_{КВИС\,j} \wedge X_{fi}) \in \Gamma^{ТЗ} \wedge \right. \\ f_{КВИС\,j}(t_{ТЦУ\,j}) \notin f_{КВИС}^{ТЗ}(t_{ТЦУ}), \text{то } f_j^{КВИС} \subset f_н, \rightarrow f_j \in \Delta_Y, \end{cases} \quad (65)$$

где Г – функция проверки ограничений $(f_{КВИСj} \wedge X_{fj})$ технологического шаблона КВИС;

$f_н$ – нештатные функции КВИС;

Δf_j – множество выявленных фактов наличия нештатных функций КВИС, являющихся признаками компьютерных атак.

Источником начальной информации для применения комбинированного метода и средств обнаружения компьютерных атак на КВИС являются данные от датчиков СПКА, условия работы которых, определяются следующим образом.

Пусть в структуре КВИС используется множество датчиков:

$$Q(t_{ТЦУ}, \mathrm{Y_A}) = \sum_{j=1}^{k} (Q_{ОПО\,k} + Q_{СПО\,k} + Q_{ЦКО\,k} + Q_{МЭ\,k}) \ge \mathrm{Q}_{КВИС}^{ТР}, \quad (66)$$

$Q_{ОПО} = Q_{ОС} + Q_{СУБД}$,

$Q_{ОПО\,k}, Q_{СПО\,k}, Q_{ЦКО\,k}, Q_{МЭ\,k}$ – множество датчиков общего и специального программного обеспечения, цифрового коммуникационного оборудования и межсетевых экранов соответственно.

И существует множество состояний и событий воздействия компьютерных атак:

$$\forall[Y_{uk}(t_{Yk})] \cup [Y_{нk}(t_{Yk})] \subset Y_A \Leftrightarrow A_k \in \{A\},$$

где $Y_{uk}, Y_{нk}$ – множества состояний известных и неизвестных атак соответственно при осуществлении событий A_k.

Тогда функция срабатывания датчиков СПКА определяется выражением:

$$F_q(t_{ТЦУ} \le t_{зад}) = \alpha_q \mathrm{P}[\mathrm{Q}(t_{ТЦУ})] \frac{\sum_{j=1}^{k} q_{cpj}}{\sum_{j=1}^{k} q_{oj}}, \quad (67)$$

а условия срабатывания датчиков имеют вид:

$$q_j(Y_{Aj}): \begin{cases} 1, \text{если } \Delta Y_{Ij} \cup \Delta Y_{Hj} \in Y_{Aj} \ge \mu_{qj} \\ 0, \text{если } \Delta \mathrm{Y}_{Ij} \cup \Delta Y_{Hj} \notin Y_{Aj} < \mu_{qj} \end{cases}, \quad (68)$$

где $1 \ge \alpha_q > 0$ – коэффициент эффективности срабатывания датчиков;

$P[Q(t_{ТЦУ})]$ – вероятность срабатывания датчиков;

q_{cpj} – количество сработавших датчиков;

q_{oj} – общее количество датчиков СПКА;

ΔY_{Ij} – множество признаков известных атак;

ΔY_{Hj} – множество признаков неизвестных атак;

μ_{qj} – порог срабатывания датчиков СПКА.

Таким образом, комбинированный метод обнаружения компьютерных атак на КВИС на основе оценки пороговых значений, времени выполнения ТЦУ и объемов

поступающей информации КВИС, функционального контроля, технологического шаблона и сигнатурного анализа позволяет сформировать условия для обнаружения известных и неизвестных атак в КВИС.

11 Метод анализа компьютерных атак на КВИС

Метод анализа компьютерных атак на КВИС предназначен для оценки характеристик атак на основе проверки подлинности (достоверности) атак и масштабов их воздействий [32-34, 36, 40, 67].

Исходные данные метода:

$Y_{A\,j}$ – множество компьютерных атак;

$t_{ан\,j}$ – время анализа атак;

$h_{YA\,j}$ – множество идентификационных параметров атаки;

J_j – характеристики сценария атаки;

$B_{Y\,j}$ – средства реализации атаки.

Алгоритм анализа компьютерных атак представлен на рисунке 21.

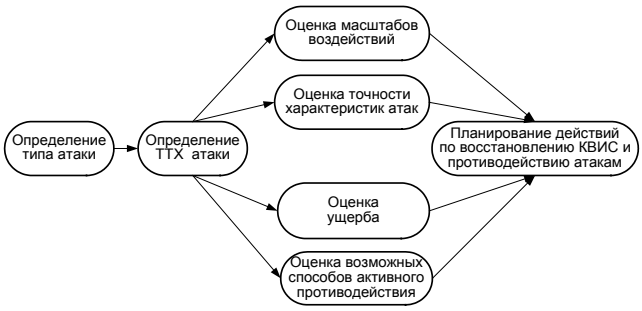

Рисунок 21 – Алгоритм анализа компьютерных атак на КВИС

В общем виде функция анализа компьютерных атак определяется выражением:

$$G_A\left(t_{AH\,j}\right) = f\left(Y_{A\,j}, h_{YA\,j}, J_j, B_{Y\,j}, A_j\right) \geq G_{ATP}, \tag{69}$$

где G_{ATP} – требуемый объем операций по анализу атак.

Метод анализа компьютерных атак на КВИС включает:

1. Определение технических характеристик атаки:

$$\begin{aligned} &\forall t_{ан\,j} \geq t_{ан}^{TP}, h_{YA\,j} \in h_{YA} \rightarrow \exists h_{YA\,j} \in \Delta_Y \,\middle|\, J_j \in J, B_{Y\,j} \in B, \\ &\Delta_Y = \left[\Delta_{Yн\,j}\left(t_{ан\,j}\right) + \Delta_{Yн\,j}\left(t_{ан\,j}\right)\right], \end{aligned} \tag{70}$$

$$f(Y_A) = \alpha_{J\,k} \frac{\sum_{j=1}^{k} \left(Y_{н\,j} + Y_{нк\,j}\right)}{\sum_{j=1}^{k} Y_{AO\,j}},$$

где $\alpha_{J\,k} = \{0.5,...,1\}$ – коэффициент, определяющий принадлежность атаки к определенному сценарию нарушителя;

$Y_{AO\,j}$ – общее количество атак.

Выявление ложных атак:

$$\forall Y_{A\,j} \in Y_A \rightarrow \exists \left(Y_{AP} \subset Y_A \wedge Y_{AЛ} \notin Y_A\right) \left| \alpha_{AЛ} \le \alpha_{ATP}, \right. \quad (71)$$

где Y_{AP} – реальные компьютерные атаки;

$Y_{AЛ}$ – ложные компьютерные атаки;

$\alpha_{AЛ} = \{0,..., N\}$ – коэффициент выявления ложной атаки.

2. Оценку масштабов воздействий компьютерных атак. Проверка масштабов воздействия атак осуществляется по сверке штатной топологии КВИС и части, подвергшейся воздействию атак:

$$S_{KBИС\,i}^{KP} \le S_{KBИС\,i}^{B3} \le S_{KBИС\,i},$$

где $S_{KBИС\,i}^{KP}$ – критическая часть топологии сети, подвергшаяся вторжению компьютерных атак, при которой нарушается деятельность функционирования КВИС;

$S_{KBИС\,i}^{B3}$ – часть топологии КВИС, на которую оказано реальное воздействие атак.

3. Оценку точности характеристик компьютерных атак методом Монте-Карло:

исходя из положений центральной предельной теоремы [1, 10] при большом числе данных для анализа $N_{Y\,ан}$ обнаруженных атак, случайная величина $\overline{h}_{YA}$ распределена по нормальному закону. Тогда вероятность того, что среднее значение h_{YA} будет отличаться от ее математического ожидания меньше, чем на ε равное:

$$P\left(\overline{h}_{YA} - m_{hYA}\right) < \varepsilon) = 2\Phi\left(\frac{\varepsilon\sqrt{N_{Y\,AH}}}{\sigma_{YA}}\right), \quad (72)$$

а статистическая оценка среднего квадратического отклонения $h_{YA\,j}$ равна:

$$\sigma_{YA} = \sqrt{\frac{1}{N_{Y\,\text{АН}}} \sum_{j=1}^{N_{Y\,\text{АН}}} h_{YA\,j} - \overline{h}_{YA\,j}^{2}} \qquad (73)$$

4. Оценку ущерба от воздействия атак, которую необходимо проводить по методике [Эл. уч. Эксп. оценка].

5. Оценку возможных способов активного противодействия атакам на основе экспертной оценки компьютерных атак и автоматизированного выбора эффективных способов активного противодействия нарушителю в соответствии с моделью раздела 12.

6. Планирование действий по восстановлению КВИС и активному противодействию атакам, которое включает в свой состав: восстановление устойчивости функционирования КВИС и оценку возможностей по активному противодействию атакам в соответствии с моделью активного противодействия компьютерным атакам.

Требование к достоверности компьютерных атак выполняется путем полноты анализа системных журналов СПКА, КВИС и средств защиты информации КВИС и детализации характеристик атак по принципу их декомпозиции:

1. Проверка данных комбинированного метода обнаружения компьютерных атак на КВИС:

– сведения, полученные анализом сигнатур атак;
– сведения, полученные анализом аномалий в КВИС;
– сведения, полученные функциональным анализом КВИС.

2. Проверка данных компонентов КВИС:

– сведения из коммуникационных структур КВИС по нарушению протоколов передачи данных (например, анализ нарушений в топологии сети при использовании протокола TCP/IP);
– сведения из информационных структур КВИС по нарушению структур баз данных, файловых систем, хранилищ данных и других элементов информационного обеспечения.

3. Проверка системных журналов СЗИ КВИС.

Эффект от применения метода заключается в получении аналитических оценок атак для проведения динамической корректировки параметров КВИС и базы данных компьютерных атак СПКА.

12 Алгоритм и модель активного противодействия компьютерным атакам

В процессе реализации предупреждения, обнаружения и анализа атак осуществляется диагностика состояния безопасности информации в КВИС, фиксация фактов атак, классификация и запись параметров в базы данных атак (пассивная составляющая).

Однако действия по блокированию источников атаки, не допущению «информационной агрессии» на КВИС и уничтожению компонентов атаки (активная составляющая) не предпринимаются. Поэтому необходимо создание математических основ активного противодействия компьютерным атакам.

Исходными положениями при разработке алгоритма активного противодействия компьютерным атакам на основе попарного сравнения компонентов и факторов противодействия являются:

- классификация видов активного противодействия компьютерным атакам;
- схема активного противодействия источникам компьютерных атак (рисунок 22);
- алгоритм активного противодействия компьютерным атакам (рисунок 23).

Виды активного противодействия компьютерным атакам классифицируются по ожидаемым результатам противодействия и делятся на два типа:

1. Блокирование точек внедрения атак в структуру КВИС и устранение компонентов атак.
2. Воздействие на источники компьютерных атак нарушителя и дезорганизация атак.

Способы и ожидаемые результаты активного противодействия компьютерным атакам представлены в таблице 10.

Таблица 10 – Способы и ожидаемые результаты активного противодействия компьютерным атакам

Виды активного противодействия	Способы противодействия (СП)	Ожидаемый результат от противодействия (РП)
1. Блокирование точек внедрения атак в структуру КВИС и устранению компонентов атак	СП11: проведение мониторинга потенциальных точек внедрения атак в структуру КВИС	РП11: предупреждение об уязвимостях КВИС и принятие мер по их устранению
	СП12: проверка подозрительных событий нарушения устойчивости функционирования КВИС и сопоставление фактов нарушений	РП12: заблаговременное выявление фактов подготовки компьютерных атак нарушителем
	СП13: выявление средствами СПКА фактов наличия компонентов атак в программах, данных и цифровом коммуникационном оборудовании КВИС	РП13: подготовка перечня компонентов атак в структуре КВИС для их уничтожения
	СП14: туннелирование и разработка дополнительных стеков протоколов передачи данных	РП14: создание дополнительных рубежей противодействия атакам за счет использования защищенных протоколов передачи данных в составе КВИС, СПКА и средств взаимодействия с СЗИ КВИС
	СП15: ограничение доступных сервисных функций программ	РП15: устранение избыточных функций программ и формирование минимума функций устойчивого функционирования КВИС
	СП16: реконфигурация и перезапуск КВИС, СПКА, СЗИ	РП16: достижение устойчивости информационно-вычислительного процесса в КВИС и надежной работы СПКА и СЗИ
	СП17: логическое блокирование точек внедрения атак на рубежах противодействия СПКА и несанкционированных абонентов средствами межсетевых экранов	РП17: недопущение несанкционированного подключения к информационным ресурсам КВИС, внедрения компонентов атак и инициализации их запуска

	СП18: уничтожение компонентов атак средствами СПКА	РП18: противодействие выводу КВИС из строя и восстановление его работоспособности
2. Воздействие на источники компьютерных атак нарушителя и дезорганизации атак	СП21: внедрение дополнительных функций управления противодействием атакам и контроля функций обмена информацией на семи уровнях протоколов передачи данных	РП21: воздействие на протоколы передачи данных и средства несанкционированного информационного взаимодействия по каналу КВИС – средства нарушителя
	СП22: перенаправление атак на ложные информационные объекты, использование ложных функций, обманных систем и «стелс» технологий ложных компонентов КВИС	РП22: дезорганизация атак нарушителя на основе применения «ложных» информационных объектов
	СП23: блокирование источников атак и средств сканирования уязвимостей путем отправки пакета передачи данных логического отключения абонента – источника атаки и средств несанкционированного сканирования уязвимостей КВИС	РП23: отключение источника атак на КВИС и его средств несанкционированного сканирования
	СП24: сканирование и анализ сетевого трафика, определение топологии объекта, схемы адресации и других параметров средств реализации компьютерных атак нарушителем	РП24: подготовка системы исходных данных об уязвимых местах и возможностях воздействия на источник атак нарушителя
	СП25: нарушение порядка передачи данных между абонентами	РП25: воздействие на коммуникационную структуру источников компьютерных атак
	СП26: нарушение целостности баз и хранилищ данных, которые используются при реализации атак на КВИС	РП26: воздействие на структуру информации источников компьютерных атак
	СП27: функциональное поражение средств нарушителя путем контроля его вычислительных ресурсов	РП22: дезорганизация атак нарушителя на основе захвата управления его вычислительными ресурсами

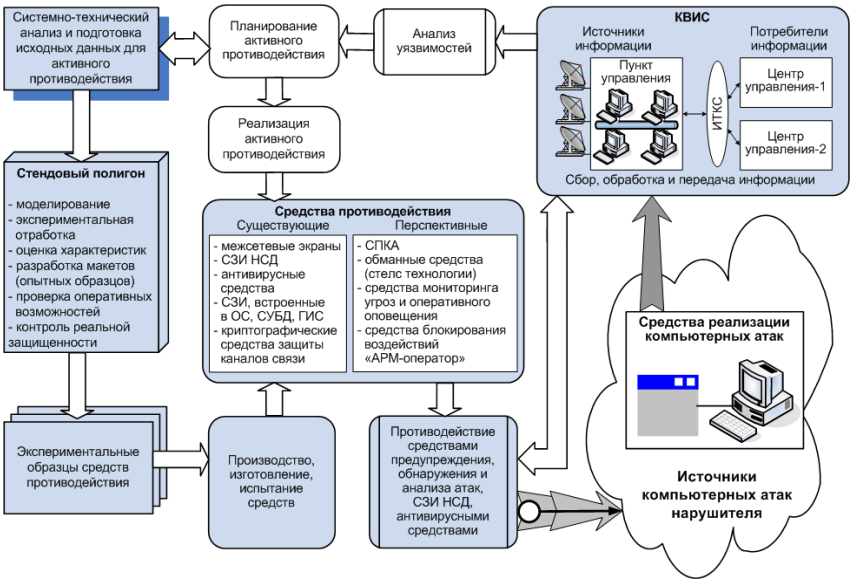

Рисунок 22 – Схема активного противодействия источникам компьютерных атак

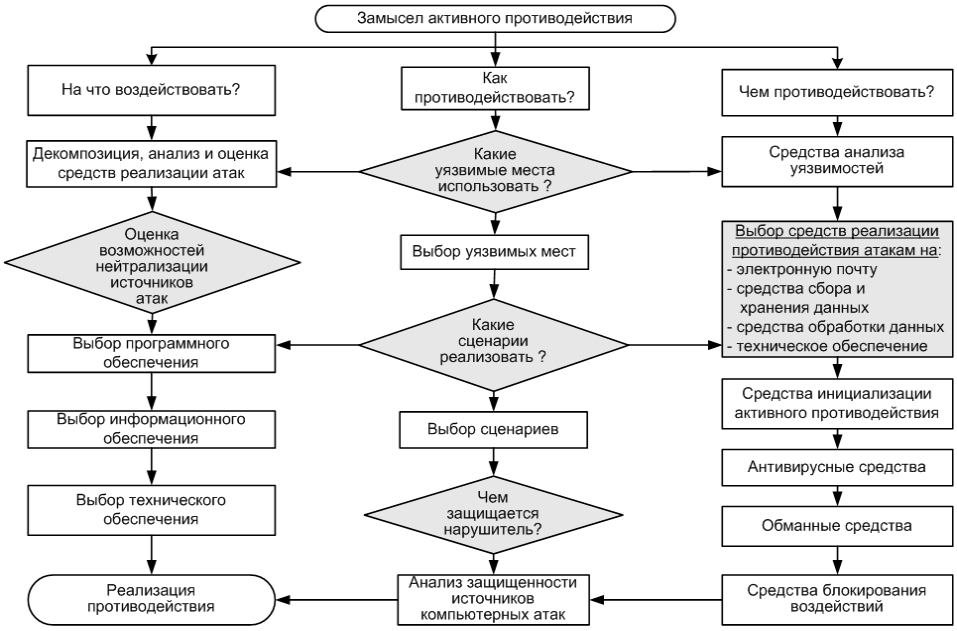

Рисунок 23 – Алгоритм активного противодействия компьютерным атакам

Математическая модель активного противодействия компьютерным атакам разработана на основе использования метода анализа иерархий [56, 57, 62, 66]. Она предназначена для принятия решений по активному противодействию при наличии факторов неопределенности – выбора сценария, средств активного противодействия атакам и анализа сложной иерархической структуры КВИС и компьютерных атак нарушителя. Метод анализа иерархий применяется в том случае, когда в условиях

неопределенности альтернативные решения нельзя увязать между собой точными линейными функциями и принятие решений осуществляется по количественным показателям предпочтений, определяемых экспертным путем.

В математической модели на основе логических правил метода анализа иерархий параметры факторов неопределенности активного противодействия компьютерным атакам интерпретируются математическими соотношениями, которые позволяют определить весовые коэффициенты факторов и оценить их значимость в процессе принятия решений. Схема модели активного противодействия компьютерным атакам представлена на рисунке 24.

Модель реализуется математическими выражениями в соответствии со следующей последовательностью шагов:

Шаг 1. Определение базовых компонентов, факторов и ограничений активного противодействия компьютерным атакам:

$$D^{(t_1)} = \left\{D_1^{(t_1)},...,D_m^t\right\}, \quad (74)$$

где D_m^t – множество основных компонентов активного противодействия, $m = 1, \ldots, N_i$.

Установлены ограничения на активное противодействие

$T_R \le T_{ПРПК}$,

где T_R – время воздействия атаки;

$T_{ПРПК}$ – время противодействия нарушителя;

$R_\gamma \le R_{доп}$,

где R_γ – количество атак;

$R_{доп}$ – допустимое количество событий, при которых атака с высокой степенью вероятности (0.95) будет обнаружена.

Шаг 2. Назначение совокупности относительных весовых коэффициентов факторов, характеризующих значимость компонентов активного противодействия в процессе принятия решения по его реализации:

$$\nu^{(t)} = \left\{\nu_1^t,...,\nu_i^t\right\}, \quad (75)$$

где $\nu^{(t)} = \{0,...,1\}$ – совокупность относительных весовых коэффициентов факторов активного противодействия, $i = 1, \ldots, N$.

В модели используется принцип иерархической декомпозиции для получения относительных весовых коэффициентов как функций времени, учитывающих динамическое изменение состояния КВИС, СПКА и СЗИ и характеристик средств реализации атак нарушителя.

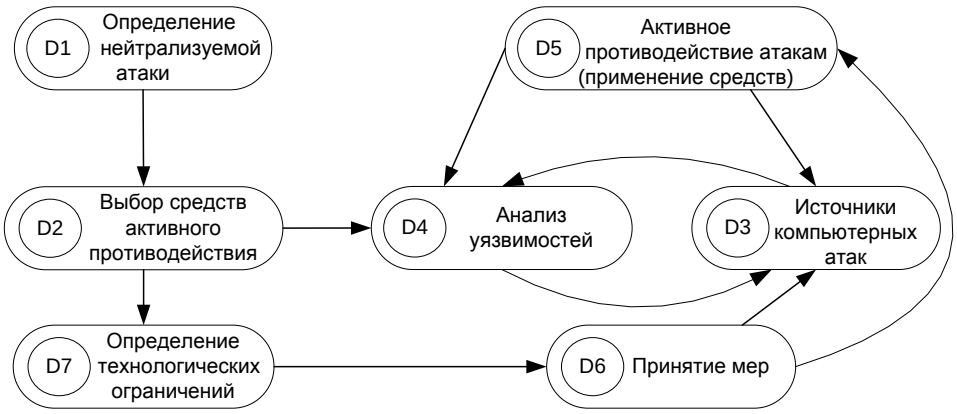

Рисунок 24 – Схема модели активного противодействия компьютерным атакам

Шаг 3. Построение обратно симметричной матрицы для попарного сравнения факторов компонентов активного противодействия:

$$W^{t}_{\text{ПРПС}} = \begin{bmatrix} 1 & \nu^{(t)}_{12} & \nu^{(t)}_{13} & \ldots & \nu^{(t)}_{1i} \\ \nu^{(t)}_{21} & 1 & \nu^{(t)}_{23} & \ldots & \nu^{(t)}_{2i} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \nu^{(t)}_{i1} & \nu^{(t)}_{i2} & \nu^{(t)}_{i3} & \ldots & 1 \end{bmatrix}. \qquad (76)$$

Определены требования к элементам матрицы

$$W^{(t)}_{\text{ПРПС}} = \left(w^{(t)}_{im}\right);\ i,m = \{1,...,N\};$$

$$w^{(t)}_{im} = \nu^{(t)};\ w_{mi} = 1/\nu;\ \nu \neq 0,$$

где $w^{(t)}_{im}$ – количественные оценки экспертами факторов компонентов активного противодействия.

Шаг 4. Проверка согласованности матрицы для попарного сравнения компонентов активного противодействия по уравнениям:

$$W_{\text{ПРПС}}^{(t)} \nu^{(t)} = \lambda \max \nu^{(t)}, \ \sum_{m=1}^{i} \nu_m^{(t)} = 1, \tag{77}$$

где $\lambda \max = i$ максимальное собственное число матрицы попарного сравнения $W_{\text{ПРПС}}^{(t)}$.

Шаг 5. Определение коэффициента превосходства одного фактора активного противодействия над другим фактором по соотношениям:

$$w_{im}^{(t)} = \frac{\nu_i^{(t)}}{\nu_m^{(t)}} > 1, \ \nu_{im}^{(t)} = \frac{\nu_i^{(t)}}{\nu_m^{(t)}}, \tag{78}$$

где $\nu_{im}^{(t)}$ – коэффициент предпочтения i-го фактора компонента активного противодействия D_i^t над m-м фактором компонента активного противодействия D_m^t из множества компонентов D^t.

Шаг 6. Принятие решений о порядке активного противодействия в условиях неопределенности по соотношениям для выбора альтернативных решений:

$$\begin{aligned} &f\left(D^{(t)}\right) \arg \max \min E_j\left(D_m^{(t)}\right), \\ &D_m^{(t)} \in D^{(t)}; m, j \in [1:N]. \end{aligned} \tag{79}$$

Базовый набор основных компонентов активного противодействия и весовые коэффициенты факторов при анализе иерархии активного противодействия приведены в таблице 12. Исходя из данных таблицы 12, многоэкстремальная задача решается путем нахождения следующих функций:

$$\begin{cases} E_1\left(D_1^{(t)}, D_2^{(t)}\right) \to \max \\ E_2\left(D_3^{(t)}\right) \to \min \\ E_3\left(D_4^{(t)}\right) \to \max \\ E_4\left(D_5^{(t)}, D_6^{(t)}\right) \to \min \\ E_5\left(D_7^{(t)}\right) \to \max \end{cases} \tag{80}$$

При выполнении условия $w_{im}^{(t)} v_i^{(t)} = \lambda \max v_i^{(t)}$ будет верно соотношение:

$$\lambda^{(t)} \max = \sum_{m=1}^{n} w_{im}^{(t)} v_m^{(t)} \geq \sum_{m=1}^{n} w_{rm}^{(t)} v_m^{(t)} = \lambda \max v_r^{(t)}, \quad (81)$$

где n – количество попарных оценок факторов компонентов активного противодействия;

i, r – оценки факторов, полученные различными экспертами.

Шаг 7. Оценка факторов активного противодействия по обобщенному весовому коэффициенту:

$$K_{\text{ПРПС}}(A_j) = \sum_{D=1}^{m} \left[\prod_{k=1}^{N} \left(v_{ks} \sum_{i=1}^{N} v_i v_{im} \right) \right], \quad (82)$$

где A_j – варианты активного противодействия;

v_{ks} – оценки факторов, полученные S-ми экспертами по критерию первого уровня иерархии принятия решений по порядку формирования активного противодействия.

В качестве частных критериев оценки экспертами D_m – факторов компонентов A_j – вариантов активного противодействия предложена таблица коэффициентов предпочтения b_i (таблица 11).

Таблица 11 – Коэффициенты предпочтения для оценки факторов активного противодействия компьютерным атакам

№ п/п	Уровень предпочтения	Значения шкалы предпочтения
1.	Низкий уровень предпочтения – b	$b_1 = 2$
2.	Средний уровень предпочтения – b^2	$b_2 = 4$
3.	Высокий уровень предпочтения – b^3	$b_3 = 8$
4.	Очень высокий уровень предпочтения – $\geq b^4$	$b_4 \geq 16$

Пример иерархии принятия решений на основе применения математической модели активного противодействия компьютерным атакам для случая работы 2-х экспертов и оценки по критериям иерархии 2-х уровней приведен на рисунке 25. Затонированные окружности с факторами D_m на рисунке 25 означают предпочтение, отданное экспертом доминирующим факторам.

На рисунке 25 приняты обозначения: D_m – компоненты активного противодействия, для оценки экспертом 1; Q_m – компоненты активного противодействия, для оценки экспертом 2.

Для попарного сравнения и оценки основных компонентов и факторов активного противодействия используются значения весовых коэффициентов таблицы 12, которые могут быть приняты в качестве базовых при выборе вариантов активного противодействия компьютерным атакам на КВИС.

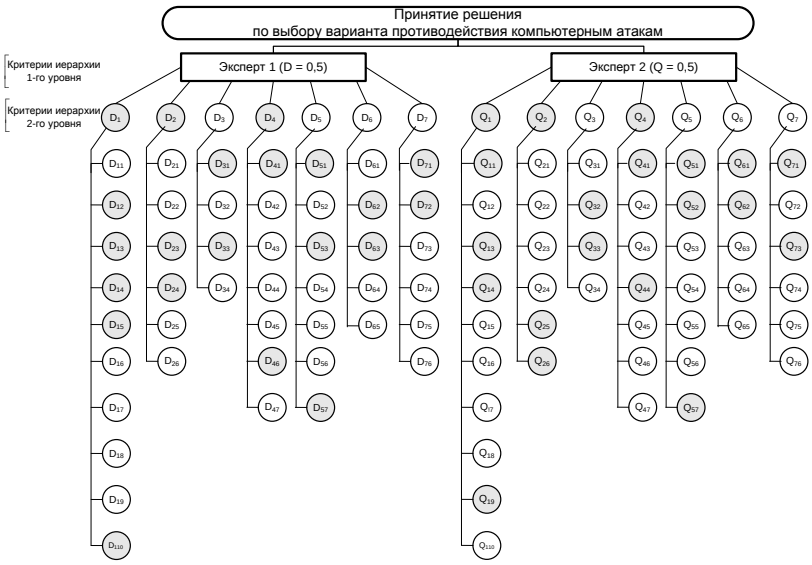

Рисунок 25 – Иерархия принятия решений по порядку активного противодействия компьютерным атакам для случая работы 2-х экспертов и оценки по критериям иерархии 2-х уровней

Таблица 12 – Основные компоненты и весовые коэффициенты факторов при анализе иерархии активного противодействия

№ п/п	Компоненты активного противодействия	Факторы активного противодействия (альтернативного выбора)	Обобщенные весовые коэффициенты факторов
1.	D_1 (Q_1) – сценарии активного противодействия $v_{k11} = 0.16$ $v_{k12} = 0.18$	1. «Ложная информация»: – искажение информации; – введение дезинформации. 2. Функциональное поражение: – нарушение режимов функционирования; – блокирование информации («отказ в обслуживании»); – разрушение (стирание информации); – перехват информации; – разглашение (утечка) информации; – хищение информации; 3. «Разрыв соединения»: – логическое отключение абонентов; – перенаправление пакетов данных (искажение порядка маршрутизации).	$v_{D11} = 0.07$ $v_{Q11} = 0.12$ $v_{D12} = 0.09$ $v_{Q12} = 0.09$ $v_{D13} = 0.16$ $v_{Q13} = 0.17$ $v_{D14} = 0.12$ $v_{Q14} = 0.12$ $v_{D15} = 0.15$ $v_{Q15} = 0.10$ $v_{D16} = 0.04$ $v_{Q16} = 0.04$ $v_{D17} = 0.05$ $v_{Q17} = 0.03$ $v_{D18} = 0.09$ $v_{Q18} = 0.08$ $v_{D19} = 0.09$ $v_{Q19} = 0.14$ $v_{D110} = 0.14$ $v_{Q110} = 0.11$
2.	D_2 (Q_2) – характеристики средств активного противодействия	1. Поражаемые источники компьютерных атак нарушителя. 2. Управление средствами активного противодействия.	$v_{D21} = 0.11$ $v_{Q21} = 0.9$ $v_{D22} = 0.12$ $v_{Q22} = 0.8$

№ п/п	Компоненты активного противодействия	Факторы активного противодействия (альтернативного выбора)	Обобщенные весовые коэффициенты факторов
	$v_{k21} = 0.23$ $v_{k22} = 0.17$	3. Среднее время необходимое для сбора информации о нарушителе. 4. Среднее время необходимое для выявления средств воздействия нарушителя. 5. Среднее время блокирования сервера баз данных нарушителя. 6. Среднее время блокирования сервера электронной почты нарушителя.	$v_{D23} = 023$ $v_{Q23} = 0.17$ $v_{D24} = 0.25$ $v_{Q24} = 0.14$ $v_{D25} = 0.15$ $v_{Q25} = 0.27$ $v_{D26} = 0.14$ $v_{Q26} = 0.25$
3.	D_3 (Q_3) – источники и средства реализации атак нарушителя $v_{k31} = 0.07$ $v_{k32} = 0.10$	$W_{СПОi}$ – вариант структуры специального программного обеспечения (СПО). $W_{ОПОi}$ – вариант структуры общего программного обеспечения (ОПО). $W_{ТОi}$ – вариант структуры технического обеспечения (ТО). $W_{ИОi}$ – характеристики информационного обеспечения (ИО).	$v_{D31} = 0.38$ $v_{Q31} = 0.23$ $v_{D32} = 0.22$ $v_{Q32} = 0.28$ $v_{D33} = 0.31$ $v_{Q33} = 0.34$ $v_{D34} = 0.09$ $v_{Q34} = 0.15$
4.	D_4 (Q_4) – уязвимые места источников и средств реализации атак нарушителя $v_{k41} = 0.18$ $v_{k42} = 0.25$	$M_{уд.ИТО}$ – уязвимости удаленного доступа. $M_{ЛВС\ ИТО}$ – уязвимости доступа к локальной вычислительной сети (ЛВС). $M_{АРМ\ ИТО}$ – уязвимости доступа к автоматизированным рабочим местам (АРМ). $M_{ОС}$– уязвимости доступа к операционной системе (ОС). $M_{СУБД}$ – уязвимости доступа к системе управления базой данных (СУБД) и базы данных (БД). $M_{СПО}$ – уязвимости доступа к СПО.	$v_{D41} = 0.22$ $v_{Q41} = 0.24$ $v_{D42} = 0.15$ $v_{Q42} = 0.12$ $v_{D43} = 0.08$ $v_{Q43} = 0.09$ $v_{D44} = 0.14$ $v_{Q44} = 0.21$ $v_{D45} = 0.13$ $v_{Q45} = 0.10$ $v_{D46} = 0.19$ $v_{Q46} = 0.14$

№ п/п	Компоненты активного противодействия	Факторы активного противодействия (альтернативного выбора)	Обобщенные весовые коэффициенты факторов
		$M_{ГИС}$ – уязвимости доступа к геоинформационной системе (ГИС).	$v_{D47} = 0.09$ $v_{Q47} = 0.10$
5.	D_5 (Q_5) – средства защиты нарушителя $v_{k51} = 0.13$ $v_{k52} = 0.12$	$M_{ВЧСi}$ – средства создания виртуальных частных сетей. $M_{НСДi}$ – методы и средства защиты информации от НСД. $M_{АВi}$ – антивирусные средства. $M_{СЗИ\ ОПОi}$ – СЗИ, встроенные в ОС, СУБД, ГИС. $M_{СГУi}$ – средства гарантированного уничтожения информации. $M_{НСКi}$ – средства защиты от несанкционированного копирования. $M_{СКЗИi}$ – средства криптографической защиты информации.	$v_{D51} = 0.25$ $v_{Q51} = 0.2$ $v_{D52} = 0.15$ $v_{Q52} = 0.23$ $v_{D53} = 0.20$ $v_{Q53} = 0.15$ $v_{D54} = 0.07$ $v_{Q54} = 0.13$ $v_{D55} = 0.06$ $v_{Q55} = 0.04$ $v_{D56} = 0.05$ $v_{Q56} = 0.05$ $v_{D57} = 0.22$ $v_{Q57} = 0.2$
6.	D_6 (Q_6) – меры и средства противодействия нарушителя $v_{k61} = 0.13$ $v_{k62} = 0.13$	$M_{МЭi}$ – средства межсетевого экранирования. $M_{СПКАi}$ – средства предупреждения и обнаружения компьютерных атак. $M_{СТi}$ – обманные системы (стелс-технологии). $M_{МУОi}$ – средства мониторинга угроз воздействия атак и оперативного оповещения. $M_{ОПi}$ – средства блокирования воздействия «АРМ – оператор».	$v_{D61} = 0.22$ $v_{Q61} = 0.25$ $v_{D62} = 0.36$ $v_{Q62} = 0.31$ $v_{D63} = 0.27$ $v_{Q63} = 0.19$ $v_{D64} = 0.10$ $v_{Q64} = 0.14$ $v_{D65} = 0.07$ $v_{Q65} = 0.09$

№ п/п	Компоненты активного противодействия	Факторы активного противодействия (альтернативного выбора)	Обобщенные весовые коэффициенты факторов
7.	D_7 (Q_7) – технологические ограничения КВИС $v_{k71} = 0.10$ $v_{k72} = 0.05$	$T_{Огрi}$ – временные ограничения на сбор, доставку, хранение и передачу информации. B – скорость передачи данных в канале связи. $V_И$ – объем передаваемой информации. $T_{ВА}$ – время информационно-логического взаимодействия абонентов сети. V_i – тип протокола передачи данных. F – совокупность функций КВИС.	$v_{D71} = 0.21$ $v_{Q71} = 0.21$ $v_{D72} = 0.23$ $v_{Q72} = 0.19$ $v_{D73} = 0.17$ $v_{Q73} = 0.25$ $v_{D74} = 0.10$ $v_{Q74} = 0.08$ $v_{D75} = 0.17$ $v_{Q75} = 0.016$ $v_{D76} = 0.12$ $v_{Q76} = 0.11$

Таким образом, разработанные алгоритм и модель активного противодействия компьютерным атакам позволяют с использованием метода анализа иерархий Т. Саати осуществить анализ динамически изменяющихся во времени факторов компонентов активного противодействия по математическим соотношениям попарного сравнения компонентов и факторов активного противодействия.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Схема существующих методов и моделей противодействия компьютерным атакам.

2. Структура методов и моделей противодействия компьютерным атакам.

3. Методическая схема противодействия компьютерным атакам (математическая формализация).

4. Обобщенный метод распознавания компьютерных атак на КВИС (алгоритм и математическая модель).

5. Алгоритм динамических процессов противодействия компьютерным атакам на КВИС.

6. Порядок идентификации состояния КВИС на основе модели противодействия компьютерным атакам на КВИС.

7. Показатели и шкала оценки противодействия компьютерным атакам. Качественные и количественные показатели (виды показателей оценки для КВИС). Уровни устойчивости функционирования КВИС.

8. Априорный метод противодействия компьютерным атакам в терминах расширенных сетей Петри.

9. Метод предупреждения компьютерных атак на КВИС.

10. Комбинированный метод обнаружения компьютерных атак на КВИС.

11. Метод анализа компьютерных атак на КВИС.

12. Активное противодействие компьютерным атакам. Алгоритм формирования.

СПИСОК ЛИТЕРАТУРЫ

1. Абчук В.А. и др. Справочник по исследованию операций/Под общ. ред. Ф.А. Матвейчука – М.: Воениздат, 1979. – 368 с.: ил.
2. Анализ решений (введение в проблему выбора в условиях неопределенности). Райфа Г. Перев. с англ., Главная редакция физико-математической литературы издательства «Наука», М.: 1977, 408 с.
3. Актуальные вопросы выявления сетевых атак. Александр Астахов. CISA. Информационный бюллетень Jet Info, № 3 (106) – Москва, 2002.
4. Бескоровайный М.М., Костогрызов А.И., Львов В.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем «КОК»: Руководство системного аналитика. – М., Вооружение. Политика. Конверсия. 2001. – 303 с., 2-е издание.
5. Береснев О.И., Ильин В.Е. Моделирование систем защиты информации на основе сетей Петри. Тезисы докладов конференции. Методы и технические средства защиты информации. СПб, 2000.
6. Бурков В.Н., Грацианский Е.В., Дзюбко С.И., Щепкин А.В. Модели и механизмы управления безопасностью. Серия «Безопасность». – СИНТЕГ, 2001, 160 с.
7. Вакка Дж. Безопасность интранет: Пер. с англ. – М.: ООО «Бук Медиа Паблишер», 1998.– 496 с.
8. Васильев А.И. Распознающие системы. 2-е изд. Справочник. Киев: Наукова думка, 1982. – 236 с.
9. Васильев В.И., Иванова Т.А., Бакиров А.А. К вопросу о выборе критериев эффективности комплексных систем безопасности//Материалы VIII Международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2006. – с. 76-79.
10. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. – М.: Наука. – 1998.– 480 с.
11. Волков И.К., Загоруйко Е.А. Исследование операций: Учеб. Для вузов. 2-е изд./Под ред. В.С. Зарубина, А.П. Крищенко. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. – 436 с.
12. Волкова В.Н., Денисов А.А. Основы теории систем и системного анализа. – С.

Петербург, изд. СПб ГТУ, 1999.

13. Вязгин В.А., Федоров В.В. Математические методы автоматизированного проектирования: Учеб. Пособие для втузов. – М.: Высш. шк., 1989. – 184 с.
14. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2–х кн., Книга 2. – М.: Энергоатомиздат, 1994.– 176 с.
15. Гостехкомиссия России. Сборник руководящих документов по защите информации от несанкционированного доступа. СИП РИА. – Москва, 1998.
16. Гостехкомиссия России. РД. Антивирусные средства. Показатели защищенности и требования по защите от вирусов. – Москва, 1998.
17. Гостехкомиссия России. РД. Программное обеспечение автоматизированных систем и средств вычислительной техники. Классификация по уровню гарантированности отсутствия недекларированных возможностей. – Москва, 1998.
18. ГОСТ Р 50922-96. Защита информации. Основные требования и определения.
19. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
20. ГОСТ Р 51275-99. Объекты информатизации. Факторы, воздействующие на информацию.
21. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем базовая эталонная модель. Часть 2. Архитектура защиты информации.
22. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения.
23. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
24. ГОСТ Р ИСО/МЭК 15408-2002. Информационные технологии. Методы и средства обеспечения безопасности. Критерии безопасности информационных технологий.
25. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. Пособие для студ. Высш. учеб. заведений/П.Н. Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.
26. Закон РФ «Об информации, информатизации и защите информации».
27. Закон РФ «О связи».
28. Информационные технологии на железнодорожном транспорте: Учеб. для вузов ж.-д. трансп./Э.К. Лецкий, В.И. Панкратов, В.В. Яковлев и др.: Под ред.

Э.К. Лецкого, Э.С. Поддавашкина, В.В. Яковлева. – М.: УМК МПС России, 2001. – 668 с.

29. Климов С.М., Сычев М.П. Система показателей безопасности программного обеспечения. Вопросы защиты информации № 1-2. ВИМИ. – Москва, 1997, с. 11-14.
30. Климов С.М., Пальчун Б.П., Сычев М.П. Структура требований к технологической безопасности программного обеспечения. Фундаментальные исследования в технических университетах. Материалы III Всероссийской научно-технической конференции, СПб., 1999, с. 131-137.
31. Климов С.М., Семенов А.Н. Проблемные вопросы и направления обеспечения безопасности информации в космических информационно-телекоммуникационных системах в условиях информационного противоборства. Сборник научных трудов. М.: Изд. «Синтег», 1999, с. 112-120.
32. Климов С.М. Методические и технологические основы мониторинга сетевых атак в информационно-телекоммуникационных системах. Известия ТРТУ. Тематический выпуск. Материалы VI Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2004. №4, с. 36-42.
33. Климов С.М. Методы и интеллектуальные средства предупреждения и обнаружения компьютерных атак на критически важные сегменты информационно-телекоммуникационных систем. Известия ТРТУ. Тематический выпуск. Материалы VII Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2005. №4, с. 25-34.
34. Климов С.М. Модель динамических процессов обнаружения компьютерных атак при сохранении устойчивости функционирования критически важных информационных сегментов. Известия ТРТУ. Тематический выпуск. Материалы VIII Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2006. №4, с. 46-55.
35. Климов С.М. Метод распознавания образов компьютерных атак. //Безопасность информационных технологий. 2007.
36. Климов С.М. Методы предупреждения, обнаружения и анализа компьютерных атак. //Приборы №6 (84). 2007.
37. Корн Г., Корн Т. Справочник по математике (для научных работников и

инженеров). Определения, теоремы, формулы. 6-е изд., стер. – СПб.: Издательство «Лань», 2003. – 832 с.

38. Костров Д.В. Рынок систем обнаружения компьютерных атак./Защита информации. Конфидент. 2002.№6.
39. Котов В.Е.Сети Петри. - М.: Наука, 1984. – 358 с.
40. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2001.– 624 с.
41. Лукацкий А.В. Мир атак многообразен. http://www.infosec.ru//press/pub_luka.html.
42. Лукашкин А.Н. Программные закладки в контексте модели угроз системам военного назначения./ Защита информации. Конфидент. 2003. №1.
43. Мак-Клар, Стюарт, Скембрей Джоэл, Курц Джордж. Секреты хакеров. Безопасность сетей готовые решения, 3-е издание.: Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 736 с.: ил.
44. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. Пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с.ил.
45. Марк Джозеф Эдварс. Безопасность в Интернете на основе Windows NT/ Пер. с англ. – М.: Издательский отдел «Русская редакция» ТОО «Chanel Trading Ltd» - 199. – 656 с.: ил.
46. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Интернет/Под научной редакцией проф. Зегжды П.Д. – СПб.: «Мир и семья – 95», 1997. – 296 с.
47. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. – 2-е изд., перераб. и доп. – М.: ДМК, 1999. – 336 с.
48. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.
49. Методы распознавания: Учеб. Пособие для вузов/А.Л. Горелик, В.А. Скрипкин. – 4-е изд., испр. – М.: Высш. шк., 2004. - 261 с.: ил.
50. Нечипоренко В. И. Структурный анализ систем (эффективность и надёжность). – М.:Сов. радио,1977.-216с.
51. Обеспечение безопасности информации в центрах управления полетами космических аппаратов/Л.М. Ухлинов, М.П. Сычев, В.Ю. Скиба, О.В. Казарин. – М.: Издательство МГТУ им. Н.Э. Баумана, 2000. – 366 с.
52. Олифер В.Г., Олифер Н.А. – Компьютерные сети. СПб.: Питер, 2001 – 672 с.,

ил.

53. Петров В.А. Системный анализ моделей защиты информации//Безопасность информационных технологий. – 1998. – №1. – С.42-46.
54. Питерсон Дж. Теория сетей Петри и моделирование систем.: Мир, 1984. 216 с.
55. Расторгуев С.П. Введение в формальную теорию информационной войны. М.: Вузовская книга, 2002. – 120 с.
56. Саати Т. Принятие решений. Метод анализа иерархий: Пер. с англ.–М.: «Радио и связь», 1993.–320 с.: ил.
57. Системный анализ и принятие решений: Словарь-справочник: Учеб. Пособие для вузов/Под ред. В.Н. Волковой, В.Н. Козлова. – М.: Высш. шк., 2004 – 616 с.: ил.
58. Скудис Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: Пер. с англ. – М.: ДМК Пресс, 2003. – 512 с.: ил.
59. Советов Б.Я. Моделирование систем: Учеб. для вузов/Б.Я. Советов, С.А. Яковлев – 4-е изд., стер. – М. :Высш. шк., 2005. – 343с.
60. Специальная техника и информационная безопасность. Учебник под редакцией В.И. Кирина. Том 1. М.: Академия управления МВД России, 2000, - 783 с.
61. Справочник по теории автоматического управления/Под ред. А.А. Красовского. – М.: Наука. Гл. ред. Физ.-мат. Лит., 1987.-712 с.
62. Таха, Хемди А. Введение в исследование операций, 7-е издание.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 912 с.: ил.
63. Теория эксперимента. Налимов В.В. Физико-математическая библиотека инженера, Изд. «Наука». Главная редакция физико-математической литературы, 1971 г., 208 с.
64. Фор А. Восприятие и распознавание образов/Пер. с фр. А.В. Серединского; под ред. Г.П. Катыса. – М.: Машиностроение, 1989. – 272 с.: ил.
65. Хоффман Л.Дж. Современные методы защиты информации. Пер. с англ. - М.: Советское радио, 1980.
66. Чернoруцкий И.Г. Методы принятия решений. СПб.: БХВ-Петербург, 2005. – 416 с.:ил.
67. Чирилло Дж. - Обнаружение хакерских атак.– СПб.:,2003.– 864 с.: ил.
68. Шикин Е.В., Чхартишвили А.Г. Математические методы и модели в

управлении: Учеб. пособие. – 3-е изд. – М.: Дело, 2004. – 440 с.

69. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006.274 с.: ил.