АДАПТИВНЫЙ МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КФС С ТОЧКИ ЗРЕНИЯ СИСТЕМНОГО ПОДХОДА

Полтавцева М.А., Зегжда Д.П.

Санкт – Петербургский политехнический университет Петра Великого,
Россия, г. Санкт-Петербург, ул. Политехническа, д.29

poltavtseva@ibks.spbstu.ru

Аннотация: В работе ставится задача адаптивного мониторинга информационной безопасности крупномасштабных киберфизических систем (КФС). Объект защиты рассматривается с точки зрения системного подхода и общей теории систем для решения задач безопасности. Автор использует иерархию системологических моделей для создания основы применения методов оценки состояния объекта защиты, определения устойчивости. Рассматривается задача систематизации структур данных мониторинга для обеспечения полноты и своевременности решения задач безопасности.

Ключевые слова: адаптивное управление, мониторинг информационной безопасности, киберфизические системы, системный анализ, универсальный решатель системных задач, управление данными.

Введение

Развитие цифровых технологий привело к появлению нового класса систем – киберфизических систем (КФС), сочетающих цифровое управление и контроль физического процесса. Проникновение цифровых технологий, в том числе – путем использования КФС, в свою очередь повлекло рост числа инцидентов безопасности и кибератак на различные сферы деятельности: медицинские системы, промышленность и т.д. [1] Широкое разнообразие КФС, их гетерогенность как в структурном, так и в технологическом плане, особенности эксплуатации усложняют задачу создания эффективных систем защиты. Непрерывные изменения в законодательной базе, расширение задач безопасности в отношении КФС также требуют непрерывного изменения систем, обеспечивающих их безопасность.

Принятие решений при обеспечении устойчивого функционирования киберфизических систем основывается на информации, поступающей в систему управления безопасностью со стороны системы мониторинга. Современным системам мониторинга информационной безопасности (МИБ) посвящено большое число работ, от архитектурных решений [2-7] до отдельных методов решения задач безопасности [8-11]. Однако, все они мало внимания уделяют обеспечению адаптивности МИБ к структурной и функциональной эволюции объекта защиты и изменяющимся условиям внешней среды, к которой относятся как информация о новых уязвимостях и угрозах, так и новые требования к обеспечению защищенности.

Для эффективного управления безопасностью КФС сегодня необходимо создание новых адаптивных систем мониторинга информационной безопасности (АМИБ), обеспечивающих информированность системы управления в условиях эволюции объекта защиты и изменений внешней среды его функционирования. Целью данной работы является формирование подхода к построению такого рода АМИБ на основе системного подхода и методологии системного анализа.

1. Адаптивный мониторинг КФС

1.1. Современная концепция мониторинга безопасности и КФС как объект защиты

Изменения в системах управления технологическими процессами, повышение степени цифровизации различных областей деятельности, рост угроз и атак на цифровые системы, а также повышение серьезности последствий таких атак [12, 13], привели к изменению подхода к мониторингу информационной безопасности. До недавнего времени МИБ выполнял задачу оценки соответствия [14], решаемую при помощи систем управления событиями безопасностью – SIEM. Сегодня этот функционал значительно расширяется, о чем говорит не только широкое создание центров управления безопасностью на основе систем мониторинга [15], но и изменения в законодательной базе [16]. Современный МИБ – это непрерывный процесс наблюдения и анализа результатов регистрации событий безопасности [16]. Цель этого процесса – выявление нарушений безопасности информации, а также гроз и уязвимостей в компьютерных системах объекта защиты.

Таким образом, для решения задачи обеспечения защищенности КФС система МИБ должна собирать и анализировать данные о самых разных аспектах объекта защиты, от функционирования отдельных объектов, до оценки КФС в комплексе и анализа внешней среды (рисунок 1).

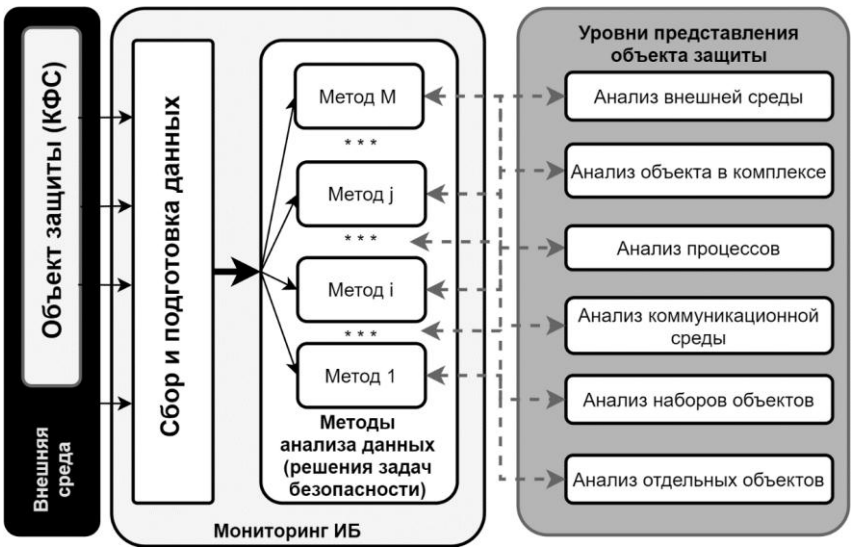

Рис. 1. Рассмотрение КФС в системе мониторинга информационной безопасности

При этом многообразие задач безопасности приводит к необходимости применения большого числа методов анализа при мониторинге. Необходимо сказать, что современные методы решения задач безопасности МИБ обладают разной эффективностью в отношении разных объектов и/или условий, что также требует оперативной коррекции их набора при внешних и внутренних изменениях и, зачастую, совместного использования нескольких методов для решения одной задачи безопасности.

Такая ситуация связана с проблемами выбора эффективного набора методов для решения задач безопасности; своевременной подготовкой данных для их применения и корректировкой наборов методов и данных при изменениях объекта и/или внешней среды. Для решение этих проблем предлагается системологический подход к адаптивному мониторингу информационной безопасности основанный на методологии системного анализа и построении взаимных отображений между задачами безопасности, методами из решения и наборами данных. В качестве основных принципов подхода декларируются принципы:

- *Целостности*: подразумевает целостное рассмотрение объекта защиты, промышленной КФС, как системы в отношении всех задач безопасности, которые должны быть реализованы над ней.
- *Конвергенции*: обуславливает необходимость соответствия системы мониторинга безопасности текущему режиму работы объекта защиты, включая пул доступных параметров, перечень задач безопасности и т.д.
- *Иерархической связности*: декларирует иерархическую декомпозицию как промышленных киберфизических систем, так и ракурсов рассмотрения объекта при адаптивном мониторинге информационной безопасности.

Киберфизическая система как объект защиты представляет собой сложную динамическую систему, плохо поддающуюся аналитическому описанию и моделированию [17]. Общая теория систем и системный подход выделяют такие свойства системы, как иерархичность, интегрированность, связность [18]. Тогда, в соответствии с уровнями рассмотрения КФС в системе мониторинга (рисунок 1) конкретизируем уровни КФС как объекта защиты – таблица 1.

Таблица 1. Уровни рассмотрения объекта защиты

Уровень системы	**Компоненты системы (примеры)**	**Технологии защиты (примеры)**
Отдельные объекты	IED – контроллер, маршрутизатор, АРМ	EDR (Endpoint Threat Detection & Response), обнаружение аномалий
Типизированные наборы объектов	IED – контроллеры заданной серии, АРМ управления подпроцессом	Обнаружение угроз (Thread Alerting), SIEM (Security Information and Event Management)
Коммуникационная среда	Сети передачи данных, SCADA - сеть	Анализ трафика и данных – NTA(Network Traffic Analysis), DLP (Data Leak Prevention)
Процессы	Управление передачей энергии, управление температурой и влажностью	Выявление угроз (Thread Hunting), SIEM

Уровень системы	Компоненты системы (примеры)	Технологии защиты (примеры)
Комплексный объект	Энергетическая сеть, оранжерея, плавильня	Thread Intelligence, анализ инцидентов безопасности
Внешняя среда	Внешние ресурсы, информация в открытых источниках, нормативно – правовые акты	Работа с угрозами (Thread Intelligence), тестирование на проникновение: Read team, Blue team.

В этих условиях задача подсистемы мониторинга информационной безопасности - обеспечение сбора и подготовки данных от объекта защиты во всех приведенных аспектах, а также предоставление и поддержка методов анализа этих данных для решения задач безопасности на всех уровнях представления объекта – от отдельных компонентов до промышленной КФС в целом с учетом контекста внешней среды с учетом конвергентности и взаимосвязей компонентов.

1.2. Управление адаптивным мониторингом информационной безопасности КФС

Для обеспечения адаптивного мониторинга в условиях изменений объекта защиты и внешней среды необходимо решить задачу взаимного отображения между задачами (целями) безопасности, методами решения и наборами данных. Боле подробно этот вопрос описан в [19, 20]. На основании этого отображения задается формальное определение схемы мониторинга $S =< (I^{Cur}, M^{Cur}, D^{Cur}), F_{IM}, F_{MD} >$ где $I^{Cur} \subseteq I = \{i_1, \dots, i_I\}$ – множество задач безопасности, определяемое однозначно на основе множества целей безопасности и используемое в рамках данной схемы; $M^{Cur} \subseteq M = \{m_1, \dots m_M\}$ – множество всех доступных методов решения задач безопасности применяемых для решения указанных задач в данный момент (в данной схеме); а $D^{Cur} \subseteq D = \{d_1, \dots d_D\}$ – соотвесвтенно множество используемых групп данных об объекте защиты. Основными этапами адаптационного процесса в системе мониторинга информационной безопасности являются:

1. Оценка состояния, включая оценку выполнения всех целей и задач безопасности и оценку условий достаточности и минимальности данных и методов для решения задачи.
2. Корректировка и фиксация множества задач безопасности.
3. Определение допустимых методов решения задач безопасности. При их отсутствии – переход на более высокоуровневую корректировку или целей безопасности, или параметров системы, включая технические возможности по сбору данных и граничные условия на основе ресурсов.
4. Формирование новой схемы мониторинга, включая оценку временных характеристик методов и подготовки данных для них, оценку всего комплекса граничных условий, решение задачи поиска оптимальной схемы мониторинга.
5. Корректировка схемы сбора и предварительной обработки данных в соответствии с новой схемой мониторинга.

Тогда адаптивность мониторинга информационной безопасности с точки зрения системного подхода и в рамках предложенных системологических принципов достигается за счет своевременной корректировки схемы мониторинга путем построения нового отображения в условиях изменившихся наборов данных, методов или задач.

Обобщенная схема адаптивного мониторинга информационной безопасности приведена на рисунке 2. Основными процессами адаптивного мониторинга являются:

1. Рабочий процесс мониторинга
    a. Определения наблюдаемых (доступных) параметров объекта защиты и их фиксация в общей модели объекта (1);
    b. Построение срезов общей модели для решения задач безопасности – фактически, подготовке наборов данных для выполнения методов (3); и их объединение в текущую общую модель при необходимости (4)
2. Процесс управления адаптивным мониторингом
    a. Определение перечня актуальных задач безопасности (2)
    b. Определение методов их решения (3.2) на основе доступных данных(3);
    c. Построение модели обработки данных и корректировка методов сбора и обработки данных при необходимости (5).

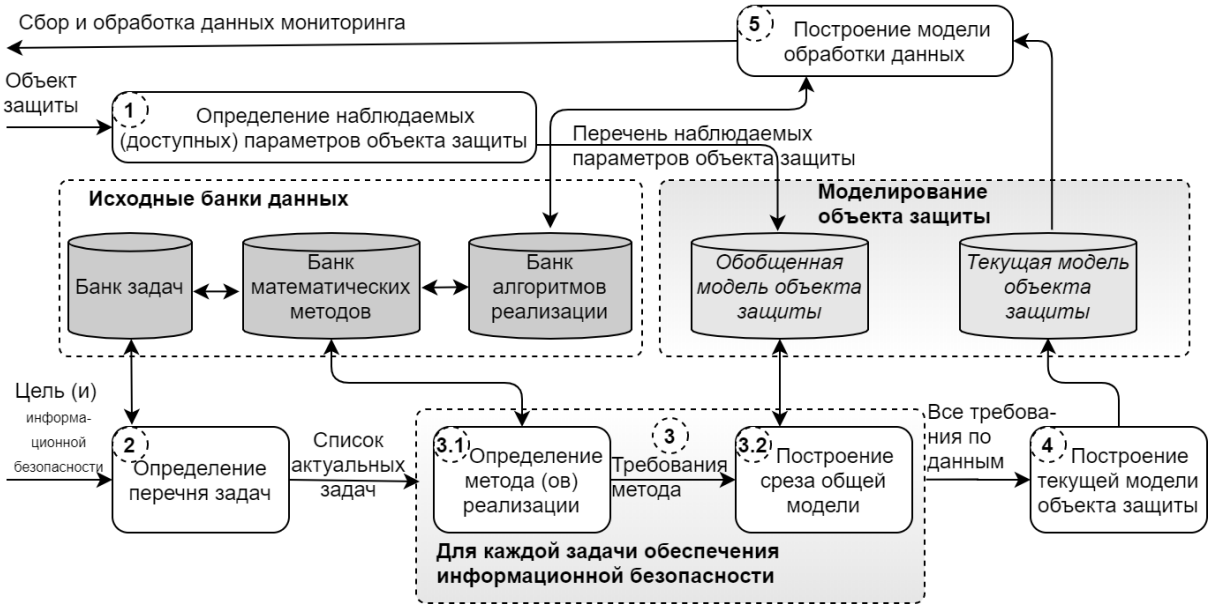

Рис. 2. Схема адаптивного мониторинга информационной безопасности

Информационной основой адаптивного мониторинга являются: внешняя база знаний, включающая банк задач безопасности, методов решения и алгоритмов их реализации в инструментах управления данными и инструментарий моделирования объекта защиты с поддержанием общей и частных моделей, которые должны быть согласованы с методами решения задач безопасности.

2. Метамодель КФС на основе универсального решателя системных задач

2.1. Применение концепции УРСЗ для построения метамодели объекта защиты

Согласование задач безопасности, методов их решения и представления (моделей) промышленной КФС как объекта защиты необходимо для обеспечения адаптивности мониторинга информационной безопасности киберфизических систем. Для его реализации предлагается использование механизма универсального решателя системных задач (УРСЗ) [21,22]. В основе универсального решателя находиться иерархия систем, представленная на рисунке 3.

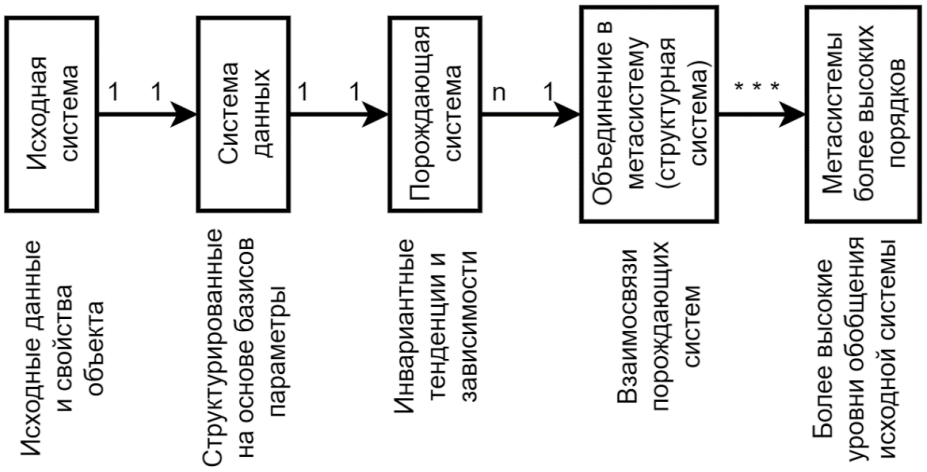

Рис. 3. Иерархия систем универсального решателя системных задач

Универсальный решатель используется для обобщения системной задачи и ее детализации для использования в отношении конкретного объекта. С точки зрения мониторинга информационной безопасности и моделирования объекта защиты УРСЗ может быть использован как методологический инструмент построения обобщенной системы моделей объекта защиты и их практического отображения в виде методологии построения модели промышленной КФС на основе данных.

Рассмотрим сопоставление систем УРСЗ с компонентами модели объекта защиты, приведенными выше. Киберфизическая система (объект защиты) представляет собой исходную систему в парадигме УРСЗ. Система данных соответствует общей модели объекта защиты, или набору всех наблюдаемых и регистрируемых параметров КФС. Порождающие системы - основной инструмент исследования

исходной системы, сопоставляются один к одному с множеством частных гипотез о функционировании промышленной КФС. Каждая такая гипотеза используется различными методами решения задач безопасности, например:

- гипотеза о фрактальной / мультифрактальной природе сетевого трафика в наборе коммуникационных связей объекта [23];
- гипотеза о самоподобном характере отдельных процессов и трафика объекта [24];
- гипотезы о функциональной зависимости между некоторыми данными, представляющими физические процессы, управляемые объектом [25] и другие.

При объединении порождающих систем в структурную (метасистему) можно говорить о построении общей модели объекта защиты для управления устойчивостью его функционирования в целом, например, на основе операций гиперграфа [26].

Приведем основные шаги исследования объекта защиты на основе системологического подхода с применением иерархии моделей в концепции универсального решателя системных задач:

1. Определение наблюдаемых параметров объекта как исходной системы УРСЗ;
2. Фиксация наблюдаемых параметров относительно базисов и формирование на основе выборки необходимых для анализа параметров базовой модели объекта защиты в соответствии с принятой парадигмой моделирования;
3. Выявление и задание извне предполагаемых свойств, трендов и закономерностей поведения отдельных параметров и наборов параметров системы;
4. Выдвижение гипотез и построение множества порождающих моделей как множества частных моделей объекта защиты;
5. Интеграция свойств и порождающих моделей с учетом их взаимосвязей и формирование структурной модели объекта защиты;
6. Формирование выводов и определение общих границ безопасного функционирования объекта.

Биективное отображение систем в системологический концепции универсального решателя системных задач и компонентов модели объекта защиты, образующее метамодель объекта защиты, приведено в таблице 2.

Таблица 2. Соответствие систем УРСЗ и компонентов модели объекта защиты

Система УРСЗ	**Компоненты модели КФС**	**Примечания**
Исходная система	Регистрируемые параметры объекта защиты	Соответствует объекту защиты с т.з. системы МИБ
Система данных	Базовая модель на основе данных	Представляет собой общую совокупность данных об объекте защиты и основу построения над-лежащих моделей
Порождающие системы	Частные модели	Соответствуют гипотезам методов решения задач безопасности и представляют собой соответствующим образом структурированные срезы данных объекта
Структурная система (метасистема)	Обобщенная модель объекта защиты	Определяется подходом к управлению устойчивым функционированием КФС в условия кибератак в целом

В силу динамических характеристик банка гипотез, а также целей анализа, структуры, числа и характеристик компонентов исходной промышленной киберфизической системы этот процесс сопровождается поддержанием обратных связей на каждом этапе с возможностью возвращения на предыдущие шаги в том случае, если не подтверждается гипотеза функционирования, возникает ситуация недостаточности данных или других аналогичных случаях (рисунок 4).

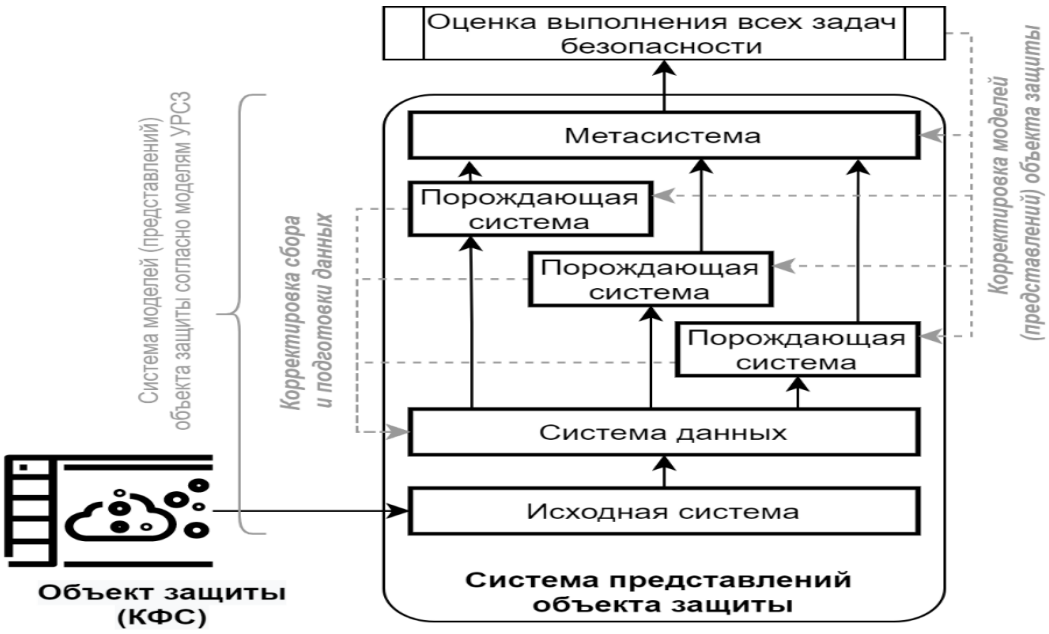

Рис. 4. Метамодель промышленной КФС при АМИБ

2.3. Моделирование КФС на основе данных

Моделирование сложных динамических систем сегодня является не простой задачей. Традиционные методы моделирования обладают такими недостатками, как требование полноты данных об объекте, отсутствие динамичности (адаптивности) модели, ограниченность в моделировании систем с высокой вариативность, ограниченная поддержка иерархий. В то же время задача АМИБ КФС накладывает такие требования, как универсальность модели, адаптивность (динамичность), поддержка иерархий, возможность представления сложных нелинейных цифровых систем в условиях неполноты информированности. Преодолеть это противоречащие позволяет моделирование на основе данных.

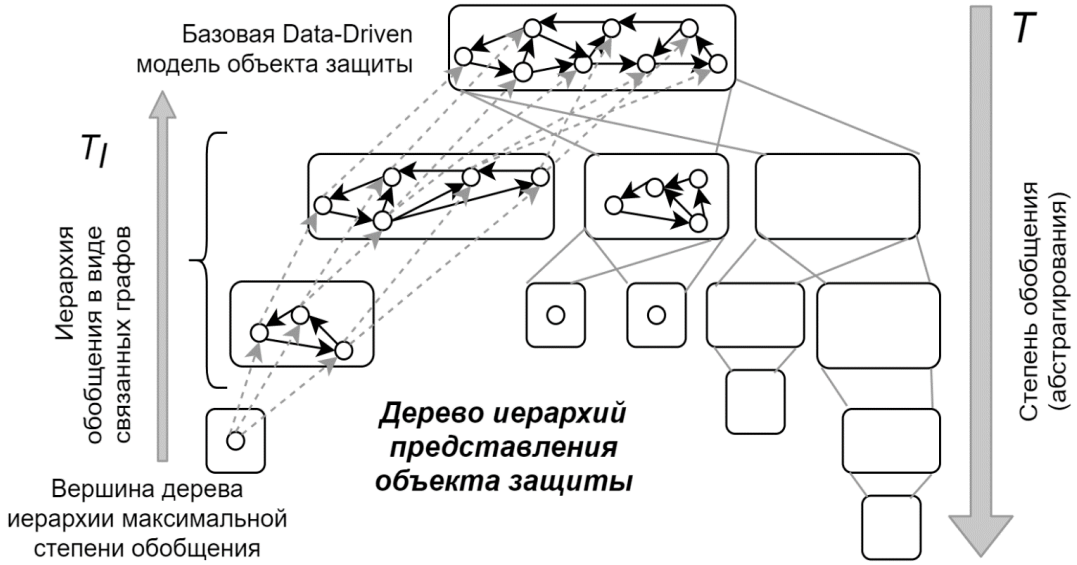

Рис. 5. Иерархия моделей на основе данных

Моделирование на основе данных, называемое также data-driven моделированием, является новым направлением имитационного моделирования, ориентированным на современные сложные системы с цифровым управлением. Особенностью моделирования является отсутствие необходимости алгоритмического представления и строгого описания системы с возможностью поддержания динамической адекватности модели [27]. Основным преимуществом моделирования на основе данных является возможность автоматизированного описания процессов и компонентов объекта моделирования, тогда как для других подходов такие описания содержат большое число ошибок.

При моделировании промышленной киберфизической системы на основе данных объект анализа представляется в виде совокупности структур данных [28]. Все процессы в объекте защиты связываются между собой через эти структуры и отношения. Базовой моделью системы является граф, вершины которого ассоциированы с компонентами КФС и представляют собой структуры данных, описывающие известную информацию о компоненте и его состоянии, а ребра - связи между компонентами системы и формируются на основе коммуникационной информации.

Каждая структурная, функциональная или иная иерархия описывающая объект защиты представляется как дерево, листами которого являются компоненты графа базовой модели на основе данных. Каждый уровень формируется путем агрегации подграфов исходной модели в узлы и формированием агрегированных связей между ними. Принципы агегации опредеяются типом иерархии. Корневой узел каждого дерева представляет собой систему (объект) в целом (рисунок 5).

3 Систематизация структур данных и обеспечение полноты АМИБ

Своевременность адаптивного мониторинга в рамках подхода обеспечивается алгоритмами выбора оптимальной схемы мониторинга, отвечающей граничным условиям по времени. Для того, чтобы была обеспеченна полнота мониторинга подсистема сбора и подготовки данных должна обеспечить исходными наборами данных все используемые методы решения задач безопасности с учетом их коррекции в процессе функционирования. Для этого необходимо определить структуры данных, востребованные методами решения задач мониторинга, и реализовать адаптивную систему их подготовки. Пример взаимного отображения задач безопасности, методов их решения и требуемых структур данных приведен на рисунке 6.

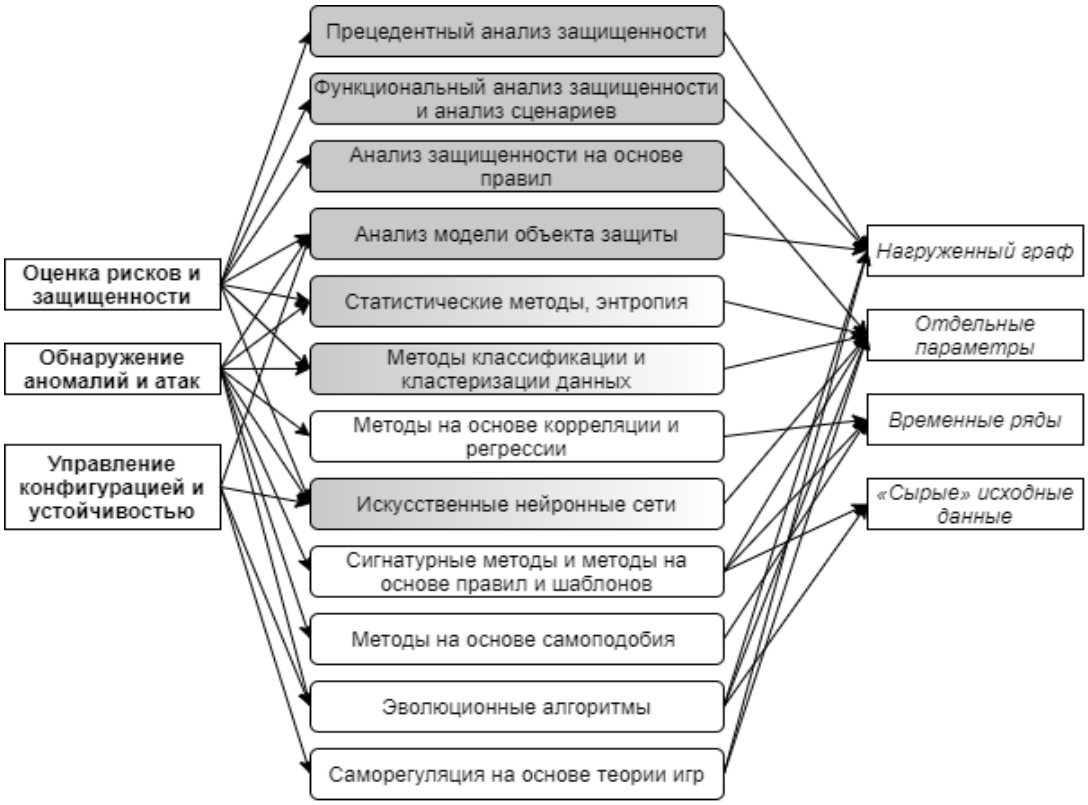

Рис. 6. Пример соответствия задач безопасности, методов их решения и структур входных данных

Все методы решения задач безопасности в системе МИБ можно разбить на несколько обобщенных групп: статистически – вероятностные методы, методы распознавания образов, методы машинного обучения, прогнозирования, интеллектуального управления и поддержки принятия решений. Особенности применения всех групп методов в рассматриваемой задаче и структуризация их входных данных приведены в таблице 3.

Тогда задача построения подсистемы сбора и подготовки данных адаптивного мониторинга информационной безопасности сводится к решению задачи выбора оптимального графа обработки данных на множестве инструментов, когда входными данными являются «сырые» сведения от объекта защиты, а результатом обработки – индивидуальные значения параметров, временные ряды

параметров (по требованию) и нагруженные графы, отражающие те или иные аспекты системы. Более подробно эта задача рассмотрена в [29]. Отображение такого графа на доступные инструменты обработки данных позволяет сгенерировать схему обработки информации конкретного объекта – КФС для заданной схемы мониторинга.

Таблица 3. Методы решения задач безопасности МИБ и структуризация входных данных

Группа методов	**Требования к применению**	**Входные данные**
Статистически-вероятностные	Известные ситуации с накопленным опытом примеров	Временной ряд
		Индивидуальные параметры
Распознавание образа		Временной ряд
		Индивидуальные параметры
Машинное обучение	Высокое качество подготовительных данных	Временной ряд
	Негибкость к изменениям	Индивидуальные параметры
Прогнозирование	Требуется высокая скорость вычислений «по требованию»	Временной ряд
Интеллектуальное управление		Нагруженный граф (гипергаф)
	Автоматизированная оценка	Индивидуальные параметры
		Временной ряд
Поддержка принятия решений		Нагруженный граф (гипергаф)
		Временной ряд

Заключение

Построение адаптивного мониторинга информационной безопасности в современных условиях является сложной задачей, в силу многообразия задач безопасности и динамических особенностей объекта защиты. Использование методологии системного подхода и теории систем позволяет сформулировать принципы мониторинга: целостность, конвергенция и иерархическая связность; обобщающие системологический подход к АМИБ.

В рамках подхода, в соответствии с принципом целостности, объект защиты – киберфизическая система – рассматривается в различных ракурсах, от отдельных компонентов до объекта в целом и характеристик внешней среды. При управлении адаптивными характеристиками мониторинга для обеспечения соответствия системы мониторинга объекту защиты и реализации принципов целостности и конвергенции используется построение взаимного отображения между задачами безопасности, методами их решения и доступными данными. На основе такого отображения определяется оптимальная схема мониторинга, включающая наборы задач, методов, данных и отображения между ними, и соответствующая граничным условиям – включая временные и иные ограничения (если такая схема вообще может быть задана в текущих условиях).

Для обеспечения данными методов решения задач безопасности на основе концепции универсального решателя системных задач задается метамодель объекта защиты, отражающая иерархию систем УРСЗ и имеющая биективное отображение с компонентами модели КФС на основе данных. Предложенные метамодель и модели соответствуют принципам целостности, конвергенции и иерархической связности. Поддержку data-driven модели, в свою очередь, реализует подсистема сбора и подготовки данных, адаптивная к изменениям в требуемых наборах выходной информации.

Литература

1. Анализ «громких» инцидентов в сфере информационной безопасности в 2019 году [Электронный ресурс] – 2020. – Режим доступа: https://www.tadviser.ru/a/498885
2. *Stevens M.* Security Information and Event Management (SIEM). Presentation // TheNEbraska CERT Conference, August 9–11, 2005. - Электронный ресурс]. – 2005. – Режим доступа: http://www.certconf.org/presentations/2005/files/WC4.pdf
3. *Котенко И.В.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (20). – СПб.: Наука. – 2012. – С. 27-56
4. *Лаврова, Д.С.* Подход к разработке SIEM-системы для Интернета вещей // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2016. – № 2. – С. 51–59.
5. *Lavrova, D.S., Zaitseva E.A., Zegzhda D.P*. Approach to Presenting Network Infrastructure of Cyberphysical Systems to Minimize the Cyberattack Neutralization Time // Aut. Control Comp. Sci. Vol.53. 2019. – P. 387–392. doi: 10.3103/S0146411619050067.

6. *Клянчин А.И. Марков А.С., Фадин А.А., Илюхин М.В*. SIEM – технология как основа построения защищенных систем // Информатизация и информационная безопасность правоохранительных органов. XXII всероссийская научная конференция. Москва – 2013. – С.270-273.
7. *Нашивочников Н.В., Лукашин А.А., Большаков А.А.* Применение аналитических средств в системе операционного мониторинга и анализа безопасности киберфизических систем для предприятий топливно-энергетического комплекса // Математические методы в технике и технологиях–ММТТ-32. – 2019. – Т. 2. – С.1-5
8. *Siddiqui S., Khan M. S., Ferens K., Kinsner W* Fractal based cognitive neural network to detect obfuscated and indistinguishable internet threats // 2017 IEEE 16th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC). 2017. – P. 297-308. doi: 10.1109/ICCI-CC.2017.8109765.
9. *Knapp, E. D., Langill J.T.* Chapter 12 - Security Monitoring of Industrial Control Systems // Editor(s): Eric D. Knapp, Joel Thomas Langill, Industrial Network Security (Second Edition). Syngress. 2015, - P. 351-386 DOI:0.1016/B978-0-12-420114-9.00012-5
10. *Jiang, Y., Yin S., Kaynak O.* Data-Driven Monitoring and Safety Control of Industrial Cyber-Physical Systems: Basics and Beyond // IEEE Access. 2018. Vol. 6. - P. 47374–47384. doi: 10.1109/ACCESS.2018.2866403
11. *Cao L.* Data Science: A Comprehensive Overview. // ACM Comput. Surv. Vol.50 Is.3. Art. 43. 2017. – P.1-42. doi: 10.1145/3076253
12. Solar JSOC Security Report. Итоги 2019 года [Электронный ресурс] – 2020. – Режим доступа: https://rt-solar.ru/upload/iblock/faf/Solar-JSOC-Security-Report-2019.pdf
13. Кибератаки на системы АСУ ТП в энергетике в Европе. Первый квартал 2020 года [Электронный ресурс] – 2020. – Режим доступа: https://ics-cert.kaspersky.ru/reports/2020/09/03/cyberthreats-for-ics-in-energy-in-europe-q1-2020/
14. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст
15. *Лукацкий А.* Измерение эффективности SOC. Часть 2 // Информационная безопасность. - №3. - 2020. [электронный ресурс] https://www.itsec.ru/articles/izmerenie-effectivnosti-soc-part-2
16. Проект стандарта «Защита информации. Мониторинг информационной безопасности. Общие положения» [Электронный ресурс] – 2020. – Режим доступа: https://fstec.ru/component/attachments/download/243
17. *Ge Z.* Review on data-driven modeling and monitoring for plant-wide industrial processes // Chemometrics and Intelligent Laboratory Systems. Vol. 171. 017. - P. 16-25, doi: 10.1016/j.chemolab.2017.09.021.
18. *Klir G. J.* Architecture of Systems Problem Solving. / N.Y.: Plenum Publishing Corporation. 1985. - 354 p.
19. *Полтавцева, М.А.* Модель активного мониторинга как основа управления безопасностью промышленных киберфизических систем // Вопросы кибербезопасности. - 2021. - № 2. - С. 51-60.
20. *Полтавцева, М.А.* Управление адаптивным мониторингом информационной безопасности КФС // Защита информации. Инсайд. - 2021. - № 3. - С. 2-8.
21. *Klir G. J.* Generalized information theory: aims, results, and open problems // Reliability Engineering & System Safety. Vol. 85. Is. 1–3. 2004. – P. 21-38. doi: 10.1016/j.ress.2004.03.003.
22. *Wang, H. Li S.* General Systems Theory and Systems Engineering //Introduction to Social Systems Engineering. Springer, Singapore. 2018. – P. 31-83. doi: 10.1007/978-981-10-7040-2_2
23. *Зегжда, П.Д., Лаврова Д.С., Штыркина А.А.* Мультифрактальный анализ трафика магистральных сетей интернет для обнаружения атак отказа в обслуживании // Проблемы информационной безопасности. Компьютерные системы. - №2. - 2018. - С. 48-58
24. *Sheluhin, O., Atayero A., Garmashev A.* Detection of Teletraffic Anomalies Using Multifractal Analysis // International Journal of Advancements in Computing Technology. Vol. 3. № 4. 2011. – P. 174-182
25. *Coletta, A.* Security Monitoring for Industrial Control Systems / A. Coletta, A. Armando // Security of Industrial Control Systems and Cyber Physical Systems. CyberICS 2015, WOS-CPS 2015. LNCS, Springer, 2015. Vol. 9588. - P. 48–62.
26. *Лаврова Д. С. Зегжда Д. П., Зайцева Е. А.* Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. – 2019. – № 2 (30). – С. 13–20.
27. *Kutz J. N.* Data-Driven Modeling & Scientific Computation: Methods for Complex Systems & Big Data OUP Oxford, 2013. – 608p.
28. *Кондратьева, Н.В., Валеев С.С.* Моделирование жизненного цикла сложного технического объекта на основе концепции больших данных // G.A. Timofeeva, A.V. Martynenko (eds.): Proceedings of 3rd Russian Conference "Mathematical Modeling and Information Technologies" (MMIT 2016). - Yekaterinburg, Russia: 2016. - С. 216-223.
29. *Полтавцева М.А.* Моделирование промышленных киберфизических систем на основе данных при мониторинге информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. - №4. - 2020. - С. 95-106