МОДЕЛЬ АКТИВНОГО МОНИТОРИНГА КАК ОСНОВА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ПРОМЫШЛЕННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Полтавцева М.А.[1]

Цель исследования. *Создание модели активного мониторинга безопасности, отвечающего требованиям современных условий для промышленных киберфизических систем.*

Метод исследования. *Используется взаимосвязь процессов мониторинга и управления безопасностью в виде набора функций мониторинга для реализации управления. Модель активного мониторинга задается с помощью тройственного отображения целей обеспечения безопасности, математических методов и данных об объекте защиты. На основе данного отображения сформулированы условия достаточности и минимальности технологических составляющих (данных и математических методов) мониторинга относительно целей и задач безопасности.*

Результаты исследования. *Разработана и представлена схема управления на основе предложенной модели активного мониторинга. Рабочий процесс включает этапы оценки, корректировки набора применяемых методов, корректировки собираемых данных и проверки достижения цели безопасности. Активный мониторинг информационной безопасности объектов цифровизации, включая промышленные киберфизические системы, позволит повысить информированность при управлении безопасностью и обеспечить требуемый уровень защиты в изменяющихся условиях.*

Ключевые слова: *безопасность киберфизических систем, активный мониторинг информационной безопасности, адаптивный мониторинг информационной безопасности, цели безопасности, задачи безопасности, предикаты соответствия, условие достижимости, условие минимальности.*

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта № 2/2020.

DOI: 10.21681/2311-3456-2021-2-51-60

Введение

Мониторинг информационной безопасности сегодня из средства оценки соответствия становится непрерывными процессом с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей. Изменение подхода к процессу мониторинга требует пересмотра его роли в управлении информационной безопасностью различных объектов информатизации

Задача обеспечения безопасности киберфизических систем (распределенных сетей интеллектуальных устройств, связанных с управлением физическими процессами) является актуальной для современной промышленности, управления процессами производства и поставок, а также целого ряда других областей [1]. Решение этой задачи невозможно без проведения комплексного и разностороннего мониторинга безопасности. Современные задачи мониторинга включают различные области, начиная от поиска и оценки угроз и заканчивая обнаружением вторжений и аудитом инцидентов информационной безопасности (ИБ).

Сегодня понятие мониторинга информационной безопасности пересматривается. До недавнего времени использовалась концепция оценки соответствия, когда под мониторингом безопасности информации понимается постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его *соответствие требованиям безопасности информации*[2]. В современных нормативно – правовых документах это понятие претерпевает изменения в сторону постоянного процесса контроля, что нашло отражение в проекте нового стандарта «Защита информации. Мониторинг информационной безопасности. Общие положения»[3] и научных работах [2,3], включая работы по стандартизации [4]. Сейчас мониторинг ИБ рассматривается как *процесс постоянного наблюдения и анализа* результатов регистрации событий безопасности *с целью выявления* нарушений безопасности информации, угроз безопасности информации и уязвимостей в информационных (автоматизированных) системах.

1 Полтавцева Мария Анатольевна, кандидат технических наук, доцент, доцент Института кибербезопасности и защиты информации Санкт-Петербургского Политехнического Университета Петра Великого, г. Санкт-Петербург, Россия. E-mail: poltavtseva@ibks.spbstu.ru ORCHID 0000-0001-9659-1244

2 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

3 Проект стандарта «Защита информации. Мониторинг информационной безопасности. Общие положения» https://fstec.ru/component/attachments/download/2438

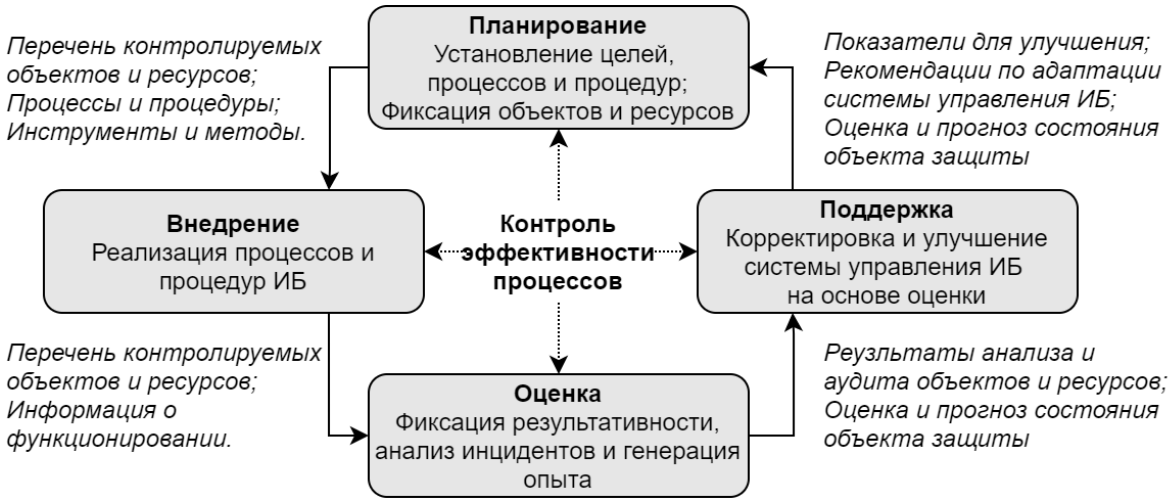

Рис.1. Основные процессы управления ИБ

Изменение подхода к мониторингу безопасности в зарубежных и отечественных исследованиях и нормативно – правовой документации приводит к необходимости пересмотра как самой концепции мониторинга ИБ, так и его места в системе управления безопасностью. Эволюция систем безопасности требует, чтобы мониторинг как постоянный процесс также трансформировался или, другими словами, обладал свойством адаптивности относительно как условий внешней среды, так и изменениям в самом объекте защиты. Таким образом, можно говорить об активном мониторинге информационной безопасности как новом этапе эволюции систем данного класса.

В данной работе рассматривается вопрос, какую роль технологический процесс современного адаптивного мониторинга безопасности играет в решении задачи управления ИБ объекта защиты. Формализуется модель адаптивного мониторинга информационной безопасности, позволяющая определить взаимосвязь основных этапов мониторинга и подзадач управления, формулируются условия достаточности и минимальности данных мониторинга относительно целей и задач безопасности.

Мониторинг информационной безопасности как основа управления кибербезопасностью

Управление информационной безопасностью – это большая системная задача. Ее выполнение (в том числе, в области современных промышленных систем) обуславливается широким спектром нормативно – правовых документов. Правовую базу сегодня составляет два федеральных закона, указы президента и ряд других положений [5], включая широкий набор государственных стандартов разной степени проработанности [6]. Сегодня это направление дополняется широким блоком документов в области защиты критической информационной инфраструктуры [7], значимую часть которой составляют промышленные системы и киберфизические системы (КФС). Дополнительно необходимо учитывать международные стандарты в области обеспечения безопасности АСУ ТП NIST SP 800-82r2 [8] и сетей промышленной коммуникации IEC 62443 [9]. Анализ нормативно – правовой базы позволяет выделить такие задачи обеспечения безопасности, как аудит ИБ, управление инцидентами и обнаружение вторжений как одни из основных.

На сегодняшний день, ни одна мера обеспечения защищенности (в частности, для КФС) не позволяет полностью предотвратить вредоносные события информационной безопасности [10]. Злоумышленниками используются как хорошо известные для корпоративных сетей, так и новы типы атак [11]. Сложность и распределенность промышленных киберфизических систем, растущее число APT – угроз, появление новых протоколов, оборудования и, как следствие, уязвимостей обуславливают наличие остаточных рисков и вероятность реализации атак «нулевого дня». Снижение вероятности ущерба при кибератаках достигается за счет решения большого комплекса задач безопасности [12,13], таких как:

- быстрое обнаружение и идентификация инцидентов ИБ;
- анализ событий и предотвращение повторных инцидентов, накопление опыта;
- планирование и координация работы систем выявления, анализа и реагирования на инциденты [14];
- минимизаций последствий инцидентов;
- сбор, хранение и анализ данных при проведении расследований инцидентов, аудит ИБ [15];
- накопление релевантного опыта по инцидентам и специфическим особенностям объекта защиты в базе знаний;
- совершенствование систем выявления, анализа и реагирования на основе накопленного опыта [15];
- осуществление активной защиты путем прекращения и предотвращения атак;
- ликвидация последствий кибератак [17].

Эти и другие задачи отражены в процессной модели управления ИБ, зафиксированной в группе международных стандартов по СМИБ (системе менеджмента информационной безопасности) [18]. Процессный подход определяет общие этапы управления безопасностью, представленные на рисунке 1.

При этом базовые четыре этапа (планирование, внедрение, оценка, поддержка) представляют собой циклический процесс, регулируемый [19,20] на основе контроля эффективности каждого из этапов. В современных цифровых системах, к которым относятся промышленные КФС, все приведенные этапы тесно связаны с процессами аудита [21] и управления инцидентами, осуществления активного противодействия [22]. Только на основе такой коллаборации может быть решен приведенный выше перечень задач [12,23]. В свою очередь задачи аудита, обнаружения вторжений и управления инцидентами в цифровой системе тесно связаны с подсистемой мониторинга безопасности (рисунок 2).

Все это позволяет позиционировать систему мониторинга безопасности киберфизических систем как технологическую основу управления безопасностью КФС, обеспечивающую поддержку различных задач безопасности и практических методов их решения. Современный мониторинг информационной безопасности должен обладать свойством адаптивности для выполнения приведенных задач безопасности. Жизненный цикл активного мониторинга как процесса включает не только этап оценки ситуации, характерный для текущих систем. Также на основе полученных и проанализированных данных определяется необходимость усиления безопасности в том или ином направлении, выбирается метод решения задачи, подбираются и подготавливаются группы данных.

Модель процесса активного мониторинга для систем управления ИБ

Рассмотрим примеры задач безопасности, применимых для промышленных киберфизических систем [1,14] и математических методов их решения [24], соотнеся математические методы с требуемыми для их работы структурами данных (рисунок 3).

Так как задачи безопасности, в большинстве случаев, соотнесены с целями в нормативно – правовой и организационно-распорядительной документации, речь

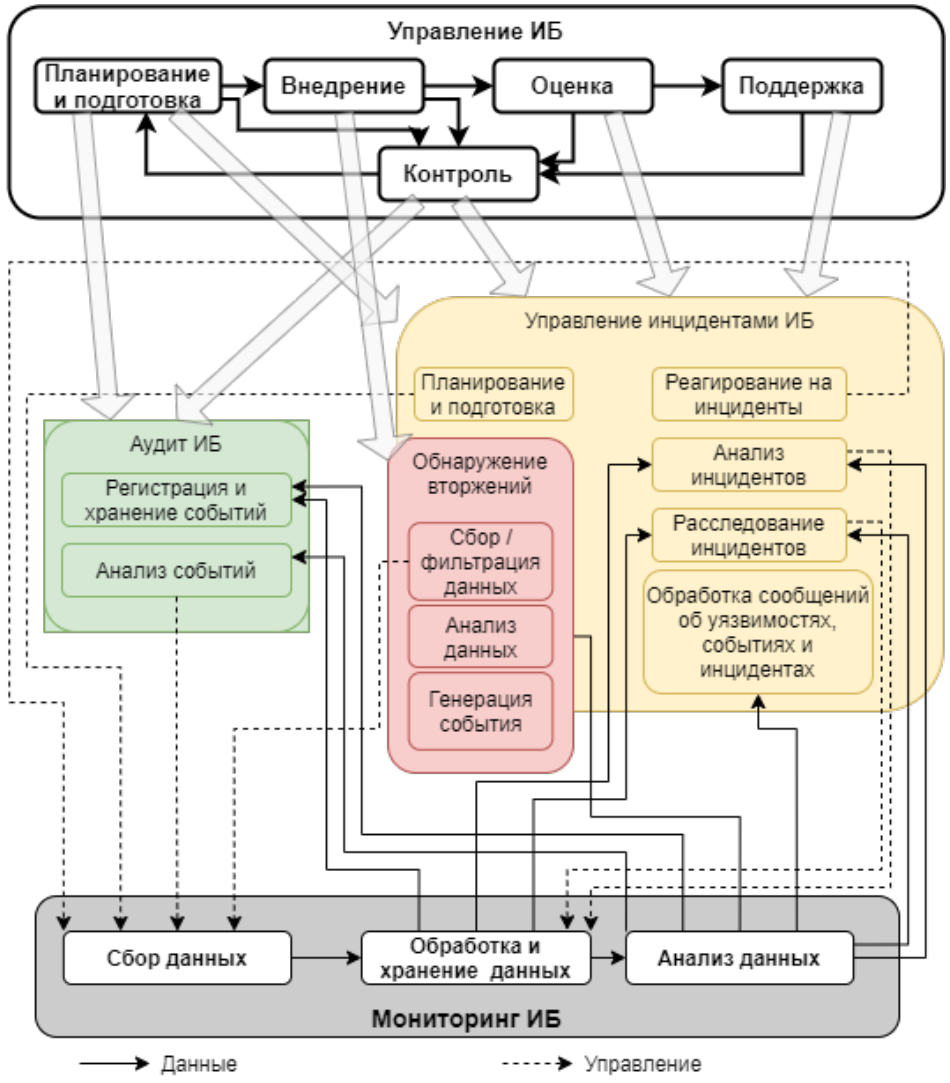

Рис.2. Связь управления информационной безопасностью КФС с подсистемой мониторинга

DOI: 10.21681/2311-3456-2021-2-51-60

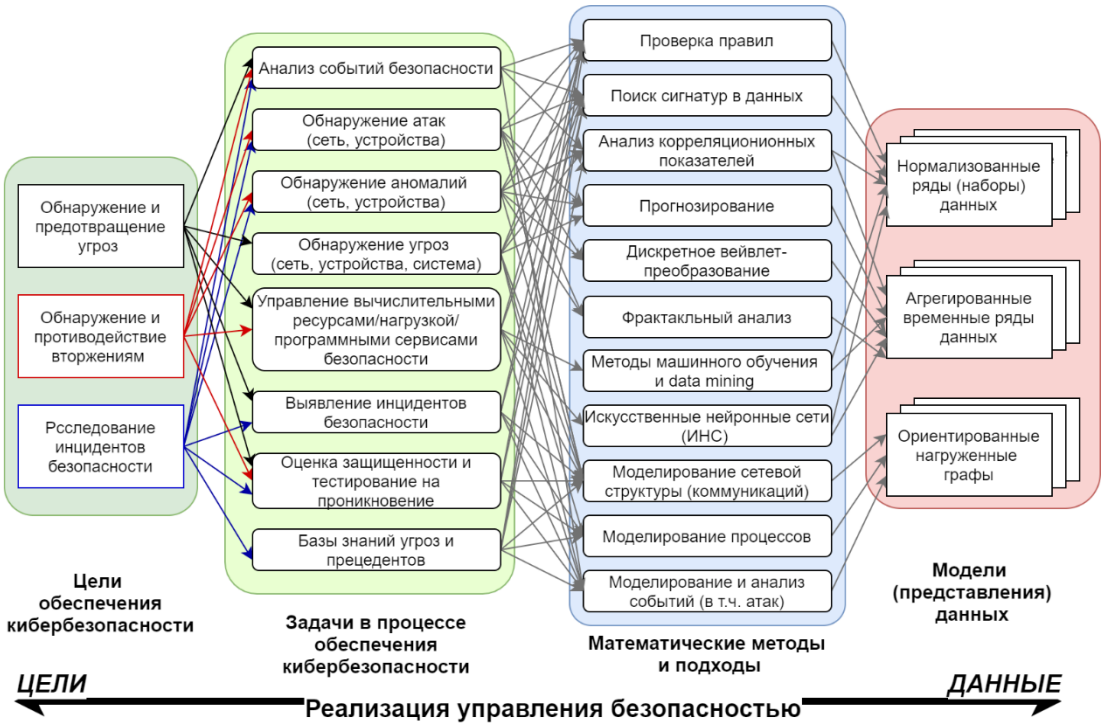

Рис.3. Пример сопоставления целей ИБ, задач безопасности, математических методов и структур данных, применяемых при мониторинге промышленных КФС

идет о построении взаимного отображения между задачами (целями) безопасности, математическими методами их решения и наборами данных, описывающих объект защиты. Под данными понимаются группы данных, которые могут быть сформированы на основе всего доступного потока информации об объекте защиты.

Для построения модели активного мониторинга как основы управления безопасностью необходимо решить две задачи. Во-первых, соотнести основные этапы мониторинга и процесса управления информационной безопасностью, формализовав их взаимосвязь. Во-вторых, определить условия выполнимости целей (задач) безопасности на основе предъявляемых ими требований к системе мониторинга и сформировать схему работы.

Система мониторинга является связующим звеном между объектом защиты и системой управления ИБ. Для решения высокоуровневых задач безопасности ей необходимо реализовать по крайней мере четыре функции.

1. Функция отображения данных мониторинга на объекты защиты и обратная ей.

$$F_o : Data \rightarrow Objects \quad (1)$$

где $Data = \{d_1,\ldots,d_n\}$ – группы данных, собираемые при мониторинге информационной безопасности объекта защиты (промышленной КФС), $Obj = \{o_1,\ldots,o_m\}$ – множество объектов (ресурсов, активов) подлежащие защите. Функция F_o^{-1} задает обратное отображение. $F_o^{-1}(o_i) = \{d_{k1},\ldots,d_{kn}\}$ представляет собой множество данных, описывающих заданный объект.

2. Функция отображения данных мониторинга на события (инциденты).

$$F_E : Data \rightarrow Events \quad (2)$$

где $Events = \{E,\ldots,E_m\}$ – множество событий, большинстве случаев – классифицированных, в терминах системы управления безопасностью объекта защиты. Функция F_E^{-1} задает обратное отображение. $F_E^{-1}(E_i) = \{d_{k1},\ldots,d_{kn}\}$ представляет собой множество данных, описывающих событие, которое может являться инцидентом безопасности.

3. Функция отображения данных мониторинга на состояние объекта защиты и обратная ей.

$$F_S : Data \rightarrow Status \quad (3)$$

где $Status = \{S,\ldots,S_m\}$ – множество состояний объекта защиты, большинстве случаев – классифицированных, в терминах системы управления безопасностью. Функция F_S^{-1} задает обратное отображение. $F_S^{-1}(S_i) = \{d_{k1},\ldots,d_{kn}\}$ представляет собой множество данных, описывающих состояние объекта защиты. Состояние объекта защиты определяется в соответствии с некоторой заданной моделью представления промышленной КФС, ассоциированной с представлениями в системе управления безопасностью.

4. Функция прогнозирования состояния объекта защиты

$$F_{SP} : (Data, Status) \rightarrow Status' \quad (4)$$

где $Status = \{S,\ldots,S_m\}$ и $Status' = \{S',\ldots,S'_m\}$ – множества состояний объекта защиты, большинстве случаев – классифицированных, в терминах системы управления безопасностью. $Status$ – исходное состояние а

$Status'$ – прогнозируемое состояние в некоторый последующий момент времени. Горизонт прогноза зависит от соответствующей задачи безопасности, а также математических методов, применяемых для генерации состояния $Status'$.

Сопряжение основных этапов мониторинга информационной безопасности на задачу и этапы управления ИБ на примере распределенной промышленной КФС с использованием основных функций мониторинга приведено в таблице 1.

Таким образом формируется взаимосвязь между задачами безопасности промышленных КФС и техническими требованиями к мониторингу безопасности. Согласование вышележащих методов и технологических методов и средств обработки данных становится ключевым аспектом для обеспечения своевременности и полноты предоставления данных и результатов мониторинга и влияет на управление безопасностью промышленных КФС в целом.

Предложенная модель позволяет сформулировать математическое представление отображений между целями обеспечения безопасности, математическими методами и группами данных [25], описывающих объект защиты (рисунок 4).

Отображение $F_{ID}: I \to D$ отображает связь целей безопасности и собираемых данных. В общем случае отображение F_{ID} и транзитивное отображение целей и определяемых ими методов решения задач безопасности $F_{IM}: I \to M$ и методов с собираемыми группами данных $F_{MD}: M \to D$ не идентичны, также как и обратные отображения $F_{ID}^{-1}: D \to I$ и $F_{IM}^{-1}: M \to I$ и $F_{MD}^{-1}: D \to M$.

Однако, не идентичность прямых отображений описывает ситуацию отсутствия необходимых математических методов или невозможность сбора необходимых данных. Обе ситуации являются неразрешимыми с практической точки зрения. Формально определим условие достаточности собираемых данных и математических методов для решения задачи следующим образом:

$$\forall (i \in I) \exists (D_i \subseteq D, M_i \subseteq M) | \\ | \left(F_{ID}(i) = D_i \wedge F_{IM}(i) = M_i \wedge F_{MD}(M_i) = D_i\right) \quad (5)$$

Нарушение **условия достаточности** собираемых данных и применяемых методов (5) возможно в двух случаях.

Во-первых, при несоответствии доступных данных: $\nexists D_i \subseteq D \,|\, \left(F_{ID}(i) = D_i \wedge F_{IM}(i) = M_i \wedge F_{MD}(M_i) = D_i\right)$ возможна ситуация, когда существующим математическим методам достижения заданной цели требуются данные, которые не могут быть представлены объектом защиты: $F_{IM}(i) = M_i \wedge F_{MD}(M_i) = D_{i1}$, $D_i \subset D_{i1} \vee \exists (d \in D_{i1} \vee d \notin D_i)$ что противоречит условию (5).

Во-вторых, при несоответствии существующих методов не существует математического метода решающего соответствующую задачу безопасности на текущих данных $\nexists M_i \subseteq M \,|\, \left(F_{ID}(i) = D_i \wedge F_{IM}(i) = M_i \wedge F_{MD}(M_i) = D_i\right)$ или $F_{IM}(i) = M_{i1} \wedge F_{MD}(M_{i1}) = D_i$, $M_i \subset M_{i1} \vee \exists (m \in M_{i1} \vee m \notin M_i)$, что противоречит условию (5).

Не идентичность обратных отображений описывает ситуацию использования математических методов, которые не способствуют достижению целей безопасности или сбора данных, не востребованных для текущего набора методов. С практической точки зрения это ситуации явного перерасхода ресурсов. Их отсутствие определяется условием минимальности.

$$\forall (d \in D) \exists (I_d \subseteq I, M_d \subseteq M) | \\ | \left(F_{ID}^{-1}(d) = I_d \wedge F_{MD}^{-1}(d) = M_d \wedge F_{IM}^{-1}(M_d) = I_d\right) \quad (6)$$

Нарушение **условия минимальности** (6) собираемых данных и применяемых методов возможно при наличии методов, не соответствующих достижению целей безопасности или аналогичных данных и возможно в следующих случаях.

Во-первых, при наличии методов, не востребованных для решения задач безопасности, исключение которых не нарушит полноты отображения F_{ID}. В этом случае нарушается обратное отображение F_{ID}^{-1} или $\nexists (M_d \subseteq M) | \left(F_{ID}^{-1}(d) = I_d \wedge F_{MD}^{-1}(d) = M_d \wedge F_{IM}^{-1}(M_d) = I_d\right)$. То есть, не существует цели безопасности для которой используется метод m, или $F_{MD}^{-1}(d) = M_{d1} \wedge F_{IM}^{-1}(M_{d1}) = I_d$ где $M_d \subset M_{d1} \vee \exists (m \in M_{d1} \vee m \notin M_d)$, что противоречит условию (6).

Во-вторых, при наличии данных, не востребованных для решения задач безопасности, исключение которых не нарушит полноты отображения F_{ID}. В этом случае нарушается обратное отображение F_{ID}^{-1} или $\nexists (I_d \subseteq I) | \left(F_{ID}^{-1}(d) = I_d \wedge F_{MD}^{-1}(d) = M_d \wedge F_{IM}^{-1}(M_d) = I_d\right)$. То есть, не существует цели безопасности для которой собираются данные d, или $F_{MD}^{-1}(d) = M_d \wedge F_{IM}^{-1}(M_d) = I_{d1}$ где $I_d \subset I_{d1} \vee \exists (i \in I_{d1} \vee i \notin I_d)$, что противоречит условию (6).

Важно отметить, что возможно построение множества отображений вида $F_{IM}^{-1}\left(F_{MD}^{-1}: D \to M\right)$, формально отвечающих условию минимальности, но оперирующих разными наборами математических методов и, следовательно, данных для достижения одного набора целей безопасности. Это обусловлено наличием множества математических методов разной степени эффективности для решения одной и той же задачи (рисунок 3).

С точки зрения эффективности для парных отображений должны быть заданы предикаты, определяющие границы требования к системе мониторинга.

$F_{IM} \Rightarrow Precision(M)$ – предикат, задающий граничные значения точности математических методов, решающих заданную задачу безопасности.

$F_{MD} \Rightarrow Timeliness(M, D)$ – предикат, задающий граничные значения скорости сбора и обработки данных, включая применение математических методов, решающих заданную задачу безопасности.

$F_{DI} \Rightarrow Capacity(D, I)$ – предикат, задающий граничные значения качества решения заданной задачи безопасности (например, стоимость ее решения) в условиях доступных данных.

Также можно сформулировать для конкретного объекта защиты задачу поиска оптимального отображения на основе определения множеств собираемых данных и методов их обработки как задачу поиска минимум

DOI: 10.21681/2311-3456-2021-2-51-60

Таблица 1

Взаимосвязь основных этапов мониторинга безопасности и управления информационной безопасностью КФС

Этапы мониторинга безопасности	**Управление безопасностью: планирование**	**Управление безопасностью: внедрение**	**Управление безопасностью: оценка**	**Управление безопасностью: поддержка**
Сбор данных мониторинга	Формирование перечня объектов и ресурсов, определение функции F_o^{-1}	Классификация и управление ресурсами на основе F_o^{-1}	Оценка достаточности данных для наблюдения за объектом и полноты контроля ресурсов на основе F_o^{-1}	Корректировка качества отображения F_o^{-1} через корректировку $Data$ – сбора данных
Предварительная обработка и хранение данных	Определение функции F_o	Контроль состояния ресурсов на основе F_o	Контроль состояния ресурсов на основе F_o, F_S, Расследование инцидентов безопасности на основе F_o^{-1}	Корректировка качества и скорости отображения F_o через корректировку методов предварительной обработки и хранения
Анализ данных мониторинга безопасности	Формирование модели атаки, определение функций F_E^{-1} и F_E Формирование модели объекта защиты и F_S	Контроль состояния объекта и событий в системе на основе F_E, F_S, F_{SP}	Анализ состояния объекта и событий в системе на основе F_E, F_S, F_{SP}, оценка полноты и достаточности контроля объекта защиты	Корректировка качества и скорости отображений F_E, F_S, F_{SP} через корректировку методов и инструментов анализа данных

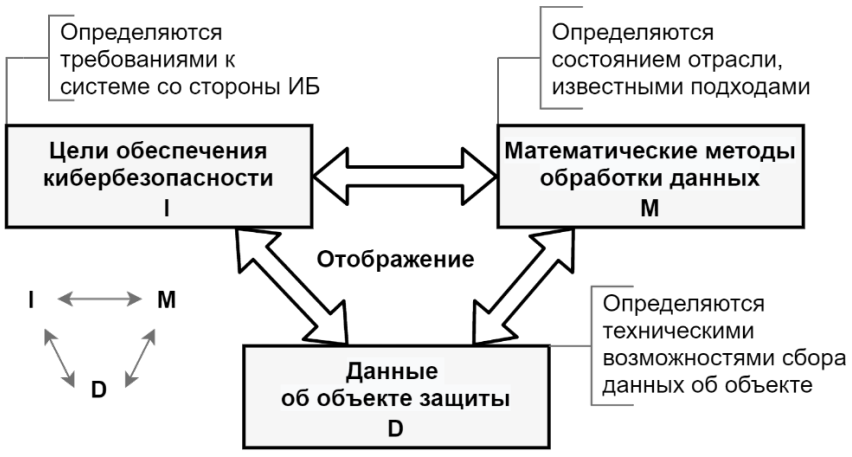

Рис.4. Тройственное отображение целей обеспечения безопасности, математических методов и данных об объекте защиты в системе мониторинга ИБ

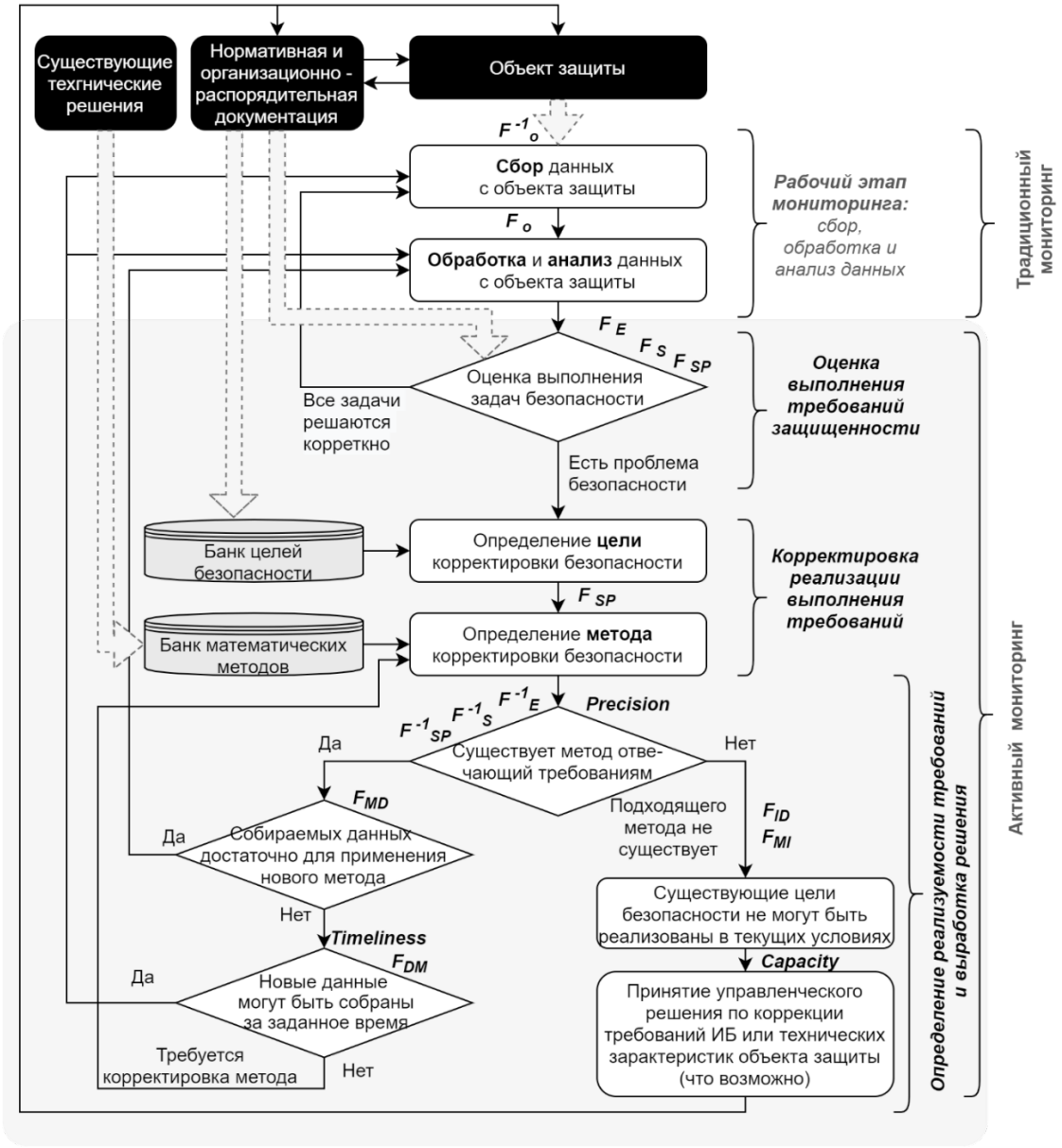

Рис.5. Схема управления на основе предложенной модели активного мониторинга

целевой функции мониторинга от некоторого набора параметров. Например, времени анализа, объема собираемых данных или стоимости.

Схема управления на основе предложенной модели

Рассмотрим схему управления на основ предложенной модели активного мониторинга. Цикл реакции на изменяющиеся условия и принятия решения состоит из следующего набора этапов:

1. Оценка.
2. Коррекция методов анализа.
3. Коррекция сбора данных.
4. Принятие решения о достижении цели.

На первом этапе анализируются данные о состоянии объекта защиты при помощи действующих математических методов, определяются инциденты безопасности, проводится оценка событий. Это основная задача системы мониторинга. На втором этапе, в случае выявления недостатков системы безопасности, угроз и т.д. производится пересмотр задач безопасности и последующая корректировка методов их решения. Этот шаг подразумевает обращение к банку целей (задач) безопасности и банку существующих математических методов.

В случае положительного решения о подборе метода, отвечающего заявленным ограничениям, переходим к третьему этапу. Иначе – технологическое состояние методов анализа не позволяет решить проблему безопасности в заданных условиях и требуется принятие управленческого решения по корректировке требований и ограничений защиты (если это возможно) или технологическому оснащению объекта защиты, для изменения условий его функционирования с целью изменения перечня задач безопасности.

DOI: 10.21681/2311-3456-2021-2-51-60

Если же один или более метод решения существует, происходит коррекция сбора данных для обеспечения его работоспособности. В этом случае также возможна ситуация практической неразрешимости задачи коррекции и обращение к условиям: требованиям или технологическому оснащения объекта. Если же все коррекции выполнены в рамках постоянного процесса мониторинга снова происходит оценка защищенности объекта и оценивается необходимость реакции. Схема управления приведена на рисунке 5.

Заключение

В работе предлагается модель активного мониторинга, служащая повышению информированности управления информационной безопасностью в современных киберфизических системах. Модель активного мониторинга включает основные функции и этапы мониторинга. Показана взаимосвязь функций мониторинга и этапов управления информационной безопасностью.

Сформулировано транзитивное замыкание трех бинарных отношений между целями (задачами) обеспечения информационной безопасности, математическими методами их решения и группами данных, представляющих объект защиты. Построение такого замыкания в условиях заданного множества целей, методов и данных позволяет гарантировать достаточность данных и математических методов для выполнения требований безопасности и исключить невостребованные данные и методы с целью экономии ресурсов в условиях заданных предикатных ограничений.

Формализованы соответствующие условия достаточности и минимальности. Выполнение условия достаточности определяет возможность практического проведения мониторинга безопасности для достижения всех заданных целей и задач безопасности. Выполнение условия минимальности позволяет исключить невостребованные методы и снизить нагрузку на мониторинг исключив сбор и обработку невостребованных для решения задач безопасности данных.

Представлена схема управления на основе модели адаптивного мониторинга безопасности, включающая основные этапы (оценка, корректировка методов и данных, принятие решения о достижении цели) выполняющиеся циклически. Определены необходимые информационные базы, такие как база целей (задач) безопасности и база математических методов их решения.

Литература

1. Zegzhda, P.D., Zegzhda, D.P. & Stepanova, T.V. Approach to the construction of the generalized functional-semantic cyber security model. Aut. Control Comp. Sci. 49, 627–633 (2015). DOI: 10.3103/S0146411615080192
2. Stephen V. Flowerday, Tite Tuyikeze, Information security policy development and implementation: The What, how and who // Computers & Security, Volume 61, 2016, Pages 169-183, DOI: 10.1016/j.cose.2016.06.002
3. S. E. Change, A. Y. Liu and Y. J. Jang, “Exploring trust and information monitoring for information security management,” 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), Shanghai, 2017, pp. 1-5, DOI: 10.1109/CISP-BMEI.2017.8302319.
4. K. Dempsey R. Niemeyer V. Y. Pillitteri R. Rudman S. Urban Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment //National Institute of Standards and Technology Special Publication 800-137A Natl. Inst. Stand. Technol. Spec. Publ. 800-137A, 78 p.– 2020 DOI:10.6028/NIST.SP.800-137A
5. Ватрушкин А. А. Правовые основы обеспечения кибербезопасности критической инфраструктуры Российской Федерации // Евразийская адвокатура. 2017. №6 (31). С. 78-84.
6. Зырянова Е.В., Белов В.М., Косов Д.Л. Применение алгоритма оценки качества нормативных правовых актов на примере оценки качества государственных стандартов в области информационной безопасности телекоммуникационных систем // Сборник научных трудов НГТУ. – 2019. – № 1 (94). – С. 132–144. – DOI: 10.17212/2307-6879-2019-1-132-144
7. Курбатов Н.М. Изменения в нормативном правовом регулировании обеспечения безопасности критической информационной инфраструктуры Российской Федерации // Вестник Удмуртского университета. Серия «Экономика и право». 2019. №3(29). С. 401-409
8. A. A. Jillepalli, F. T. Sheldon, D. C. de Leon, M. Haney and R. K. Abercrombie, “Security management of cyber physical control systems using NIST SP 800-82r2,” 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, 2017, pp. 1864-1870, DOI: 10.1109/IWCMC.2017.7986568
9. Björn Leander, Aida Čaušević, and Hans Hansson. 2019. Applicability of the IEC 62443 standard in Industry 4.0 / IIoT. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES ‘19). Association for Computing Machinery, New York, NY, USA, Article 101, 1–8. DOI: 10.1145/3339252.3341481
10. I. Jamai, L. Ben Azzouz and L. A. Saïdane, “Security issues in Industry 4.0,” 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 2020, pp. 481-488, DOI: 10.1109/IWCMC48107.2020.9148447.
11. G. Rong-xiao, T. Ji-wei, W. Bu-hong and S. Fu-te, “Cyber-Physical Attack Threats Analysis for UAVs from CPS Perspective,” 2020 International Conference on Computer Engineering and Application (ICCEA), Guangzhou, China, 2020, pp. 259-263, DOI: 10.1109/ICCEA50009.2020.00063
12. Липатников В.А., Ложечкин А.А., Шевченко А.А. Построение комплексной защиты киберфизической системы от деструктивных воздействий // Информационные системы и технологии. 2020. № 6 (122) С. 112-120
13. Левшун Д.С., Гайфулина Д.А., Чечулин А.А., Котенко И.В. Проблемные вопросы информационной безопасности киберфизических систем // Информатика и автоматизация. Т. 19. № 5. 2020. С. 1050-1088. DOI: 10.15622/ia.2020.19.5.6.

14. Vasiliev, Y.S., Zegzhda, P.D. & Zegzhda, D.P. Providing security for automated process control systems at hydropower engineering facilities. Therm. Eng. 63, 948–956 (2016). DOI:10.1134/S0040601516130073
15. Zegzhda, D.P., Lavrova, D.S. & Pavlenko, E.Y. Management of a Dynamic Infrastructure of Complex Systems Under Conditions of Directed Cyber Attacks. J. Comput. Syst. Sci. Int. 59, 358–370 (2020). DOI:10.1134/S1064230720020124
16. Konoplev, A.S., Kalinin, M.O. Tasks of providing information security in distributed computing networks. Aut. Control Comp. Sci. 50, 669–672 (2016). DOI:10.3103/S0146411616080101
17. Zegzhda, D.P., Pavlenko, E.Y. Digital Manufacturing Security Indicators. Aut. Control Comp. Sci. 52, 1150–1159 (2018). DOI:10.3103/S0146411618080333
18. Martins B.F., Serrano L., Reyes J.F., Panach J.I., Pastor O., Rochwerger B. (2020) Conceptual Characterization of Cybersecurity Ontologies. In: Grabis J., Bork D. (eds) The Practice of Enterprise Modeling. PoEM 2020. Lecture Notes in Business Information Processing, vol 400. Springer, Cham. pp 323-338 DOI:10.1007/978-3-030-63479-7_22
19. Ильина О. П., Сотавов А. К. Архитектурное моделирование системы информационной безопасности // ТТПС. 2019. №2 (48). С. 30-37.
20. Путивцев М. Е. Анализ систем управления информационной безопасности с использованием процессного подхода // Известия ЮФУ. Технические науки. 2008. №8.С. 41-47.
21. Бурлов В. Г. Разработка модели управления процессом обеспечения информационной безопасности киберфизических систем / В. Г. Бурлов и др.// Информационные технологии и системы: управление, экономика, транспорт, право.– 2019.– № 4 (36).– С. 94-98
22. X. Lyu, Y. Ding and S. Yang, “Safety and security risk assessment in cyber-physical systems,” in IET Cyber-Physical Systems: Theory & Applications, vol. 4, no. 3, pp. 221-232, 9 2019, DOI: 10.1049/iet-cps.2018.5068.
23. Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, Mohamad Malli Cyber-physical systems security: Limitations, issues and future trends // Microprocessors and Microsystems, Volume 77, 2020, 33p DOI: 10.1016/j.micpro.2020.103201.
24. Zegzhda, D.P., Pavlenko, E.Y. Digital Manufacturing Security Indicators. Aut. Control Comp. Sci. 52, 1150–1159 (2018). DOI:10.3103/S0146411618080333
25. V. Belenko, V. Chernenko, V. Krundyshev and M. Kalinin, “Data-driven failure analysis for the cyber physical infrastructures,” 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS), Taipei, Taiwan, 2019, pp. 1-5, DOI: 10.1109/ICPHYS.2019.8854888.

ACTIVE MONITORING MODEL AS A BASIS FOR SECURITY MANAGEMENT OF INDUSTRIAL CPS

Poltavtseva M.[4]

Purpose of the article *– creating a model of active security monitoring that meets the current conditions for industrial cyber-physical systems.*

Methods *of the study. The work concretizes the relationship between monitoring and security management processes in the form of a set of monitoring functions for the management implementation. The active monitoring model is defined using a threefold mapping of security goals, mathematical methods, and security object data. Based on this mapping, the paper formulates the reachability and minimality conditions of monitoring technological components (data and mathematical methods) with respect to security purposes and tasks.*

Results *of the study. The article contains a management and control scheme based on the proposed active monitoring model. The workflow includes steps to evaluate, adjust the set of methods used, adjust the data collected, and verify that the security purpose has been achieved. Active monitoring of information security of digitalized objects, including industrial cyber-physical systems, will increase awareness in security management and provide the required level of protection in changing conditions.*

The reported study was funded by Russian Ministry of Science (information security), project number 2/2020.

Keywords: *information security, security of cyber-physical systems, active monitoring of information security, adaptive monitoring of information security, security purposes, security tasks, information security management, compliance predicates, reachability condition, minimality condition*

4 Maria Poltavtseva, Ph.D., Associate Professor, Institute of Cybersecurity and Information Protection, St. Petersburg Polytechnic Peter the Great University, St. Petersburg, Russia. E-mail: maria.poltavtseva@ibks.spbstu.ru

References

1. Zegzhda, P.D., Zegzhda, D.P. & Stepanova, T.V. Approach to the construction of the generalized functional-semantic cyber security model. Aut. Control Comp. Sci. 49, 627–633 (2015). DOI:10.3103/S0146411615080192
2. Stephen V. Flowerday, Tite Tuyikeze, Information security policy development and implementation: The What, how and who // Computers & Security, Volume 61, 2016, Pages 169-183, DOI:10.1016/j.cose.2016.06.002
3. S. E. Change, A. Y. Liu and Y. J. Jang, "Exploring trust and information monitoring for information security management," 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), Shanghai, 2017, pp. 1-5, doi: 10.1109/CISP-BMEI.2017.8302319.
4. K. Dempsey R. Niemeyer V. Y. Pillitteri R. Rudman S. Urban Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment //National Institute of Standards and Technology Special Publication 800-137A Natl. Inst. Stand. Technol. Spec. Publ. 800-137A, 78 p.– 2020 DOI:10.6028/NIST.SP.800-137A
5. Vatrushkin A. A. Pravovye osnovy obespecheniya kiberbezopasnosti kriticheskoj infrastruktury Rossijskoj Federacii // Evrazijskaya advokatura. 2017. №6 (31). S. 78-84.
6. Zyryanova E.V., Belov V.M., Kosov D.L Primenenie algoritma otsenki kachestva normativnykh pravovykh aktov na primere otsenki kachestva gosudarstvennykh standartov v oblasti informatsionnoi bezopasnosti telekommunikatsionnykh sistem // Sbornik nauchnyh trudov NGTU. – 2019. – № 1 (94). – S. 132–144. – DOI: 10.17212/2307-6879-2019-1-132-144.
7. Kurbatov N.M. Izmeneniya v normativnom pravovom regulirovanii obespecheniya bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii // Vestnik Udmurtskogo universiteta. Seriya «Ekonomika i pravo». 2019. №3(29). S. 401-409
8. A. A. Jillepalli, F. T. Sheldon, D. C. de Leon, M. Haney and R. K. Abercrombie, "Security management of cyber physical control systems using NIST SP 800-82r2," 2017 *13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Valencia, 2017, pp. 1864-1870, doi: 10.1109/IWCMC.2017.7986568
9. Björn Leander, Aida Čaušević, and Hans Hansson. 2019. Applicability of the IEC 62443 standard in Industry 4.0 // IIoT. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). Association for Computing Machinery, New York, NY, USA, Article 101, 1–8. DOI:DOI:10.1145/3339252.3341481
10. I. Jamai, L. Ben Azzouz and L. A. Saïdane, "Security issues in Industry 4.0," 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 2020, pp. 481-488, doi: 10.1109/IWCMC48107.2020.9148447.
11. G. Rong-xiao, T. Ji-wei, W. Bu-hong and S. Fu-te, "Cyber-Physical Attack Threats Analysis for UAVs from CPS Perspective," 2020 International Conference on Computer Engineering and Application (ICCEA), Guangzhou, China, 2020, pp. 259-263, doi: 10.1109/ICCEA50009.2020.00063
12. Lipatnikov V.A., Lozhechkin A.A., SHevchenko A.A. Postroenie kompleksnoj zashchity kiberfizicheskoj sistemy ot destruktivnyh vozdejstvij // Informacionnye sistemy i tekhnologii. 2020. № 6 (122) S. 112-120
13. Levshun D.S., Gajfulina D.A., CHechulin A.A., Kotenko I.V. Problemnye voprosy informacionnoj bezopasnosti kiberfizicheskih sistem // Informatika i avtomatizaciya. T. 19. № 5. 2020. S. 1050-1088. DOI: 10.15622/ia.2020.19.5.6.
14. Vasiliev, Y.S., Zegzhda, P.D. & Zegzhda, D.P. Providing security for automated process control systems at hydropower engineering facilities. Therm. Eng. 63, 948–956 (2016). DOI:10.1134/S0040601516130073
15. Zegzhda, D.P., Lavrova, D.S. & Pavlenko, E.Y. Management of a Dynamic Infrastructure of Complex Systems Under Conditions of Directed Cyber Attacks. J. Comput. Syst. Sci. Int. 59, 358–370 (2020). DOI:10.1134/S1064230720020124
16. Konoplev, A.S., Kalinin, M.O. Tasks of providing information security in distributed computing networks. Aut. Control Comp. Sci. 50, 669–672 (2016). DOI:10.3103/S0146411616080101
17. Zegzhda, D.P., Pavlenko, E.Y. Digital Manufacturing Security Indicators. Aut. Control Comp. Sci. 52, 1150–1159 (2018). DOI:10.3103/S0146411618080333
18. Martins B.F., Serrano L., Reyes J.F., Panach J.I., Pastor O., Rochwerger B. (2020) Conceptual Characterization of Cybersecurity Ontologies. In: Grabis J., Bork D. (eds) The Practice of Enterprise Modeling. PoEM 2020. Lecture Notes in Business Information Processing, vol 400. Springer, Cham. pp 323-338 DOI:10.1007/978-3-030-63479-7_22
19. Il'ina O. P., Sotavov A. K. Arhitekturnoe modelirovanie sistemy informacionnoj bezopasnosti // TTPS. 2019. №2 (48). S. 30-37.
20. Putivcev M. E. Analiz sistem upravleniya informacionnoj bezopasnosti s ispol'zovaniem processnogo podhoda // Izvestiya YUFU. Tekhnicheskie nauki. 2008. №8.S. 41-47.
21. Burlov V. G. Razrabotka modeli upravleniya processom obespecheniya informacionnoj bezopasnosti kiberfizicheskih sistem / V. G. Burlov i dr.// Informacionnye tekhnologii i sistemy: upravlenie, ekonomika, transport, pravo.– 2019.– № 4 (36).– S. 94-98
22. X. Lyu, Y. Ding and S. Yang, "Safety and security risk assessment in cyber-physical systems," in IET Cyber-Physical Systems: Theory & Applications, vol. 4, no. 3, pp. 221-232, 9 2019, DOI: 10.1049/iet-cps.2018.5068.
23. Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, Mohamad Malli Cyber-physical systems security: Limitations, issues and future trends // Microprocessors and Microsystems, Volume 77, 2020, 33p DOI: 10.1016/j.micpro.2020.103201.
24. Zegzhda, D.P., Pavlenko, E.Y. Digital Manufacturing Security Indicators. Aut. Control Comp. Sci. 52, 1150–1159 (2018). DOI:10.3103/S0146411618080333
25. V. Belenko, V. Chernenko, V. Krundyshev and M. Kalinin, "Data-driven failure analysis for the cyber physical infrastructures," 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS), Taipei, Taiwan, 2019, pp. 1-5, DOI: 10.1109/ICPHYS.2019.8854888.