ПРОБЛЕМНЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ АНАЛИТИЧЕСКИХ СРЕДСТВ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ ПРЕДПРИЯТИЙ ТЭК

Нашивочников Н.В.[1], Большаков А.А.[2], Николашин Ю.А.[3], Лукашин А.А.[4]

Рассматриваются вопросы применения методов и технологий анализа данных для обеспечения безопасности киберфизических систем на предприятиях топливно-энергетического комплекса. Обозначены отличительные особенности и выделены ключевые направления применения аналитических средств системы операционного мониторинга и анализа безопасности киберфизических систем объектов критической информационной инфраструктуры. Сформулированы проблемные вопросы, определены возможности и ограничения средств расширенной аналитики в решении задач обеспечения безопасности киберфизических систем на предприятиях топливно-энергетического комплекса. Описаны архитектурные решения платформы расширенной аналитики кибербезопасности. Представленные результаты основаны на анализе информации из открытых источников: материалы научно-практических конференций, аналитических и технических обзоров по тематике безопасности индустриальных систем, и обобщения практического опыта разработки, внедрения и поддержки комплексных систем обеспечения безопасности на предприятиях топливно-энергетического комплекса.

Ключевые слова: *практики анализа данных, выявление аномалий, SIEM, платформа расширенной аналитики, машинное обучение, импортозамещение, система операционного мониторинга и анализа*

DOI:10.21681/2311-3456-2019-5-26-33

1. Введение

Киберфизические системы (cyber-physical systems (CPS)) – системы, имеющие в своем составе датчики (sensors), воздействующие на внешний физический мир исполнительные устройства (actuators) и компьютер (cyber-, кибер-, управляющую часть), который обеспечивает управление работой всей системы. Предприятия топливно-энергетического комплекс (ТЭК) давно оснащаются CPS, логика работы которых полностью определяется программным обеспечением. Для четвертой промышленной революции (Индустрия 4.0) характерно развитие сложных сетеёмких (network-intensive) систем интеграцией CPS, обычно разных производителей. Пример такой сетевой системы – CPS, функционирующие в составе единой газотранспортной сети крупного предприятия (корпорации).

Рост сложности взаимодействующих индустриальных CPS и важность безопасности их функционирования, особенно на объектах критической информационной инфраструктуры (КИИ) [1], обусловливают актуальность эффективной системы операционного мониторинга и анализа (СОМА), предназначенной выявлять и выполнять анализ событий и инцидентов безопасности в основных и обеспечивающих процессах ТЭК. Причем, СОМА создается как компонент ситуационных центров уровней предприятия, корпорации или отрасли. Ситуационные центры решают задачи комплексного обеспечения промышленной, экологической и информационной безопасности (ИБ) объектов ТЭК с целью минимизации рисков возникновений аварийных и чрезвычайных ситуаций, ликвидации последствий таких ситуаций. Одно из наиболее актуальных направлений применения аналитических средств (АС) СОМА – автоматизация проактивного мониторинга: выявление и прогнозирование аномалий в функционировании технологических объектов и индустриальных систем управления (Industrial Control System (ICS)).

Под АС понимаются практики анализа данных: соответствующий научно-методический аппарат (дисциплины) и обеспечивающие его реализацию технологии (инструментальные средства) [2]. Для оценки безопасности функционирования CPS необходим комплексный анализ с использованием практик расширенного анализа данных. Комплексность позволяет учесть степень взаимного влияния различных компонентов и систем, выявлять скрытые причинно-следственные связи и добиться синергетического эффекта в обеспечении стабильности технологических процессов (ТП). Под расширенной ана-

1 Нашивочников Николай Васильевич, заместитель генерального директора – технический директор, CISSP, ООО «Газинформсервис», г. Санкт-Петербург, Россия. E-mail: cto@gaz-is.ru

2 Большаков Анатолий Афанасьевич, кандидат технических наук, начальник отдела технологий анализа, ООО «Газинформсервис», г. Санкт-Петербург, Россия. E-mail: bolshakov-a@gaz-is.ru

3 Николашин Юрий Александрович, руководитель разработки отдела технологий анализа, ООО «Газинформсервис», г. Санкт-Петербург, Россия. E-mail: nikolashin-y@gaz-is.ru

4 Лукашин Алексей Андреевич, кандидат технических наук, доцент кафедры «Телематика (при ЦНИИ РТК)», Санкт-Петербургский политехнический университет Петра Великого, г. Санкт-Петербург, Россия. E-mail: alexey.lukashin@spbstu.ru

литикой[5] понимается исследование данных или контента с использованием сложных методов и инструментов за пределами традиционных методов бизнес-аналитики (Business Intelligence (BI))[6], чтобы находить более глубокие идеи, делать прогнозы или давать рекомендации. Практики расширенной аналитики включают себя такие дисциплины, как машинное обучение (machine learning), сопоставление образцов (pattern matching), прогнозирование (forecasting), визуализация (visualization), интеллектуальный анализ данных / текста (data/text mining), сетевой и кластерный анализ (network and cluster analysis), многомерная статистика (multivariate statistics), анализ графов (graph analysis), обработка сложных событий (complex event processing), нейронные сети (neural networks).

2. Безопасность CPS как предмет мониторинга и анализа

Важно отметить, что COMA не заменяет мониторинг ТП в контуре диспетчерского управления объектами ТЭК. Кроме этого, у COMA и ICS/SCADA (Supervisory Control And Data Acquisition) разное функциональное назначение. Отличительные особенности COMA:

1. В COMA безопасность функционирования CPS предприятий анализируется по трем связанным направлениям одновременно и в интегрированном виде: анализ сенсорных данных, ИТ-метрик и событий ИБ (рис. 1).
2. Максимальная независимость COMA от программного обеспечения ICS/SCADA, т.е. инвариантность к алгоритмам управления ТП, реализованным в индустриальных приложениях конкретных производителей.
3. Минимальное влияние COMA на КИИ: контур мониторинга безопасности функционирования ICS/SCADA независим от контура диспетчерского управления и систем автоматического управления ТП. Для функций мониторинга ситуационных центров выделяются отдельные вычислительные и телекоммуникационные ресурсы.
4. Для интероперабельности ICS/SCADA и COMA исходными данными для оценивания стабильности (устойчивости) ТП являются сенсорные данные и сигналы управления ТП низкого уровня (direct access (DA)) из OPC–сервера SCADA согласно стандарту OPC DA.

В силу киберфизической природы традиционных средств защиты информации для индустриальных CPS недостаточно. Более того, известные практики обеспечения ИБ требуют адаптации из-за системных ограничений, исторического опыта создания и развития сегмента ICS/SCADA изолированно от корпоративной сети и сети Интернет. Подробно особенности архитектурных решений обеспечения ИБ ICS/SCADA отражены, например, в [3-7].

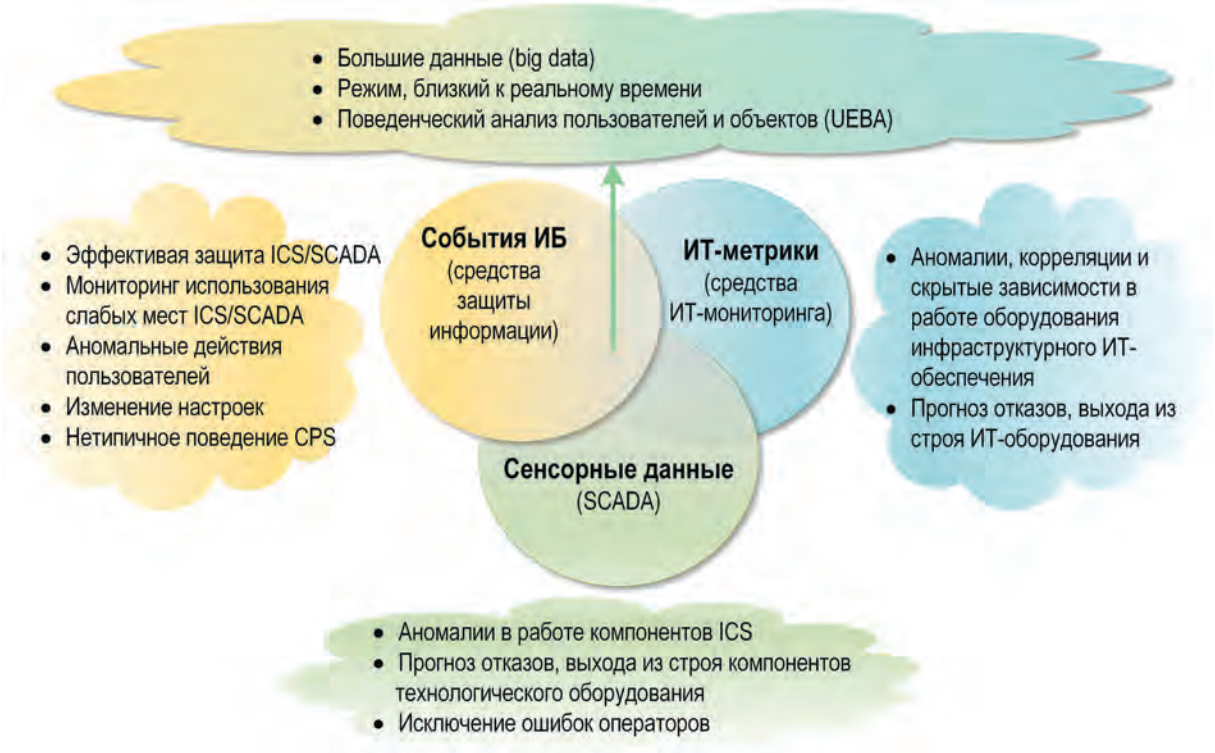

Рис. 1. Комплексный анализ безопасности CPS

5 Advanced Analytics // Gartner IT Glossary. URL: https://www.gartner.com/it-glossary/advanced-analytics/

6 С характеристикой методов BI и областью их применения можно ознакомиться по ссылке https://en.wikipedia.org/wiki/Business_intelligence

Ключевые направления применения АС в части ИБ ICS/SCADA:

1. Повышение эффективности процесса обеспечения защиты ICS.
2. Мониторинг использования слабых мест SCADA:
   - эксплойт уязвимостей SCADA;
   - отсутствие аутентификации/авторизации, вшитые пароли, скрытые учетные записи;
   - небезопасные разрешения файлов (чтение/выполнение для всех пользователей);
   - повреждение памяти (переполнение буфера);
   - открытость к инъекциям вредоносного кода.
3. Анализ взаимодействия с системами SCADA – выявление аномальных действий пользователей, изменений настроек и нетипичного поведения CPS.

Ключевые направления применения АС в части ИТ-мониторинга:

1. Поиск аномалий, корреляций и скрытых зависимостей в работе оборудования инфраструктурного обеспечения.
2. Прогнозирование отказов, выхода из строя оборудования с целью оптимизации его технического обслуживания и ремонта.

В СОМА объектов ТЭК число контролируемых сигналов ICS/SCADA достигает десятков и сотен тысяч, которые генерируют поток до нескольких миллионов измерений ежесуточно. Обработка таких потоков данных ICS для выявления и визуализации аномальных значений в режиме, близком к реальному времени, относится к классу задач «больших данных» (big data) [8-10]. В указанных работах [8-10] дан обзор большого числа современных публикаций с результатами применения различных математических моделей и методов прикладной статистики для обработки данных многомерных временных рядов и машинного обучения для автоматической классификации аномальных данных ICS/SCADA, что свидетельствует об актуальности задачи мониторинга стабильности ТП путем выявления аномальных данных датчиков ICS/SCADA.

Таким образом, к ключевым направлениям применения АС в части безопасности и устойчивости ТП относятся следующие.

1. Поиск аномалий в работе компонентов ICS, в ТП.
2. Прогнозирование отказов, выхода из строя компонентов технологического оборудования с целью оптимизации технического обслуживания и ремонта оборудования;
3. Исключение ошибок оператора.

Согласно исследованиям [11], ошибки операторов, наблюдающих и управляющими ТП, вызывают 40 % аварий. Это связано с развитием малолюдных технологий автоматизации производства. Оператор, не находясь рядом с реальным оборудованием, не имеет возможности оценить его физическое состояние в текущий момент времени и в текущих условиях эксплуатации. Выявление аномального поведения операторов, ТП, процессов ICS/SCADA обусловливают актуальность применения АС класса поведенческой аналитики пользователей и объектов (User and Entity Behavior Analytics (UEBA)) [12,13], которые призваны снять ограничения, присущие формальным правилам корреляции традиционных систем управления информацией и событиями безопасности (Security Information and Event Management (SIEM)) [14].

3. Практический опыт применения АС

С учетом перечисленных в предыдущем разделе особенностей был выполнен пилотный проект СОМА сегмента магистральной газокомпрессорной станции на основе интеграции платформ ИТ-мониторинга MicroFocus Operations Bridge, MicroFocus ArcSight SIEM и аналитической платформы Qlik Sense Enterprise. В рамках опытной эксплуатации с помощью АС обнаружены следующие типы аномалий:

- отклонения ТП, связанные с периодами смены режимов;
- переводы контуров управления в ручной режим;
- ситуации, обусловленные некорректными показаниями датчиков.

Выявлены сложные инциденты безопасности:

- предупреждение аварийного останова ТП из-за отключения источника бесперебойного питания сервера SCADA;
- определение причины частых предупредительных сигналов SCADA основного ТП, связанных с перебоями в электропитании.

Как наиболее эффективные для раннего оповещения об опасных ситуациях, обнаружения аномалий и их интерпретации эксплуатирующей организацией были признаны статистические методы выявления аномалий, модели деревьев отказов, методы визуального анализа (разведки) в интерактивном режиме на основе ассоциативной модели данных в оперативной памяти (in-memory). Эти методы не поддерживаются SCADA.

Было отмечено, что АС наиболее востребованы во время испытаний и настройки совместного функционирования CPS на этапах опытной эксплуатации, ввода в строй и начала эксплуатации новых и модернизируемых объектов. Как перспективное направление применения АС указаны задачи выявления аномального поведения операторов, объектов управления ICS и процессов работы SCADA.

Наряду с положительными результатами, следует указать на выявленные проблемы технологической и методологической готовности АС к промышленному применению.

1. Особенности данных CPS:
   - большое количество источников данных, их большой объем и разнообразие: десятки тысяч тегов сигналов, высокая частота обновления тегов до 10 раз в секунду, зашумленность и пропуски данных;
   - отсутствие ассоциации технологических данных с нормативно-справочной и конфигурационной информацией;
   - отсутствие единого стандарта (механизма) извлечения данных из SCADA разных производителей.
   - репрезентативные выборки данных, тем более размеченные наборы данных (data sets), отсутствуют.

Указанные особенности затрудняют непосредственное применение методов машинного обучения, в част-

ности, нейросетевых моделей [15-17]. Для применения методов расширенной аналитики данные должны быть предварительно подготовлены. Разработка соответствующих процедур предварительной обработки (Extract, Transform, Load (ETL)) занимает 80% проектного времени аналитика (инженера) данных [1].

2. Проблема сложности объектов мониторинга и анализа. Для достоверного предсказания событий и инцидентов безопасности нет математических моделей объектов, включая формализованных моделей физических процессов, которые адекватно описывают признаки нормального функционирования CPS. Сложность и стоимость построения математических моделей сравнима с созданием ICS/SCADA.
3. Проблема технико-экономического обоснования АС. Заинтересованность потенциальных заказчиков в АС невысокая из-за сложности получения оценок технико-экономической эффективности. Соответствующие методики отсутствуют. При этом, очевиден негативный фактор дополнительной ответственности и нагрузки на эксплуатирующий персонал, связанный с внедрением новых АС. Заказчику нужен четко выраженный (желательно в рублях, часах или в натуральных единицах сэкономленных материалов), значимый экономический или технический эффект.
4. Проблема государственного регулирования. В нормативных актах регуляторов по безопасности объектов КИИ не предусмотрены конкретные требования по комплексному анализу функционирования ICS/SCADA в части выявления аномалий.
5. Проблема импортозамещения. Российские платформы для исследовательского анализа больших данных индустриальных CPS, необходимые для успешного применения АС СОМА в промышленном масштабе, отсутствуют. Характеристика промышленных платформ, обеспечивающих поддержку практик расширенной аналитики и процессов полного жизненного цикла АС, представлена в обзорах Gartner [13,19,20].

4. Архитектура платформы расширенной аналитики безопасности

Из-за разнообразия данных и аспектов анализа требуется комплекс моделей машинного обучения. В этой связи актуально создание универсальной платформы расширенной аналитики безопасности (Advanced Security Analytics Platform (ASAP)) для автоматизации процессов выбора оптимальных моделей, циклов их обучения и доставки в среду эксплуатации для обработки потоков данных в режиме, близком к реальному времени. Архитектурная схема такой платформы представлена на рис. 2.

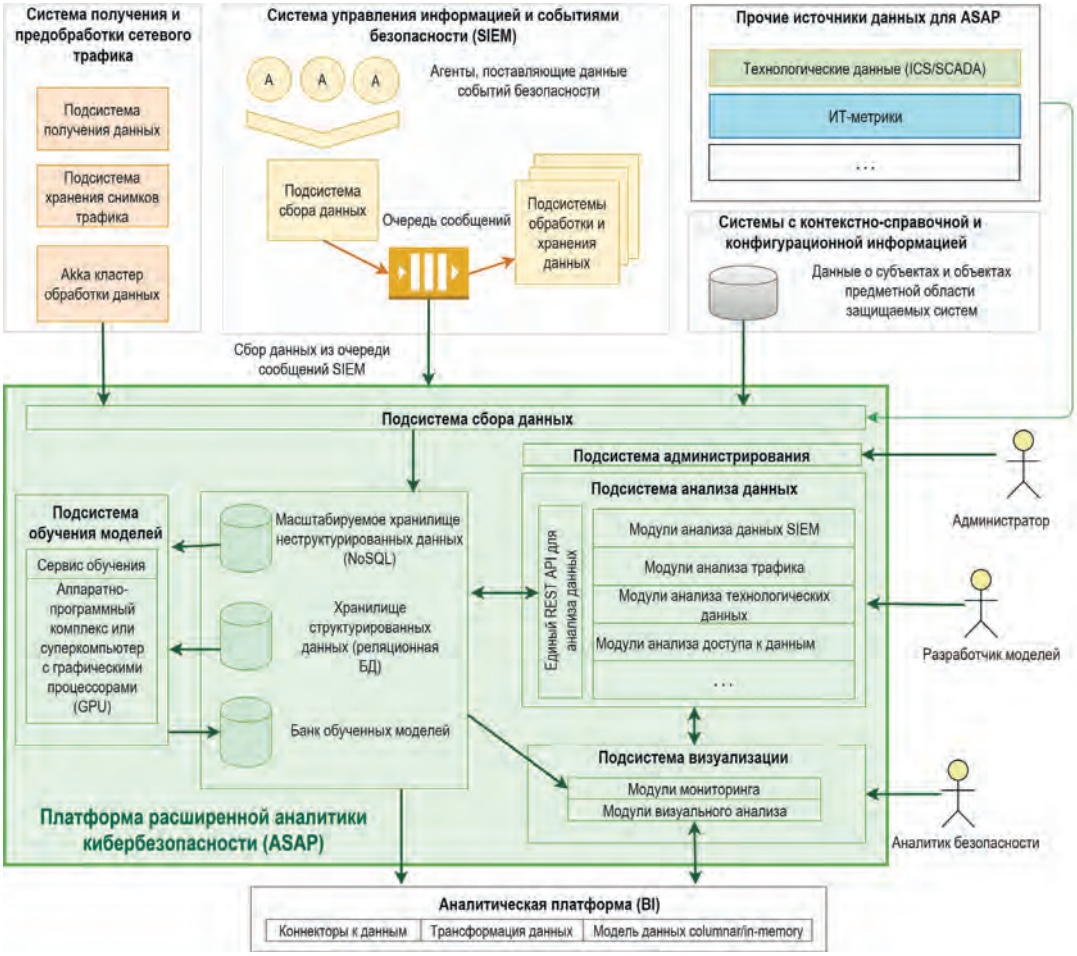

Рис. 2. Архитектура ASAP

Платформа содержит три уровня для работы с данными (рис. 3):

1. На уровне сбора данных реализуются процессы сбора, получения и предварительной обработки данных от таких систем как SIEM, ICS/SCADA, анализа сетевого трафика и другие процедуры для обработки контекстно-справочной и конфигурационной информации.
2. На уровне хранения реализуются процессы консолидации и долговременного хранения данных, полученных на уровне сбора.
3. На уровне визуализации данных реализуются процессы по построению аналитических дашбордов, интерактивных графиков и диаграмм, предоставляющих пользователю платформы возможность базового анализа консолидированных данных из различных источников.

фейса (фреймворк Angular). Стек технологий анализа данных/машинного обучения основан на экосистеме Python 3.x (scikit-learn, pandas, numpy и т.п.).

5. Заключение

Исходя из практики системной интеграции по созданию комплексных систем безопасности предприятий ТЭК, показаны место и назначение АС в COMA CPS, сформулированы проблемные вопросы методологической и технологической готовности АС к промышленному применению. Раскрыты результаты применения практик расширенной аналитики для реального объекта ТЭК:

1. Комплексный подход к анализу соответствует требованиям многоаспектного мониторинга безопасного функционирования объектов ТЭК, позволяет определить степень взаимного влияния отдельных компонентов.
2. АС обеспечивают решение задач проактивного мониторинга, которые в настоящее время не реализованы в ICS/SCADA.
3. При вводе в эксплуатацию и в начале эксплуатации технологических объекта, когда наблюдается наибольшее число аномалий в интегрируемых CPS,

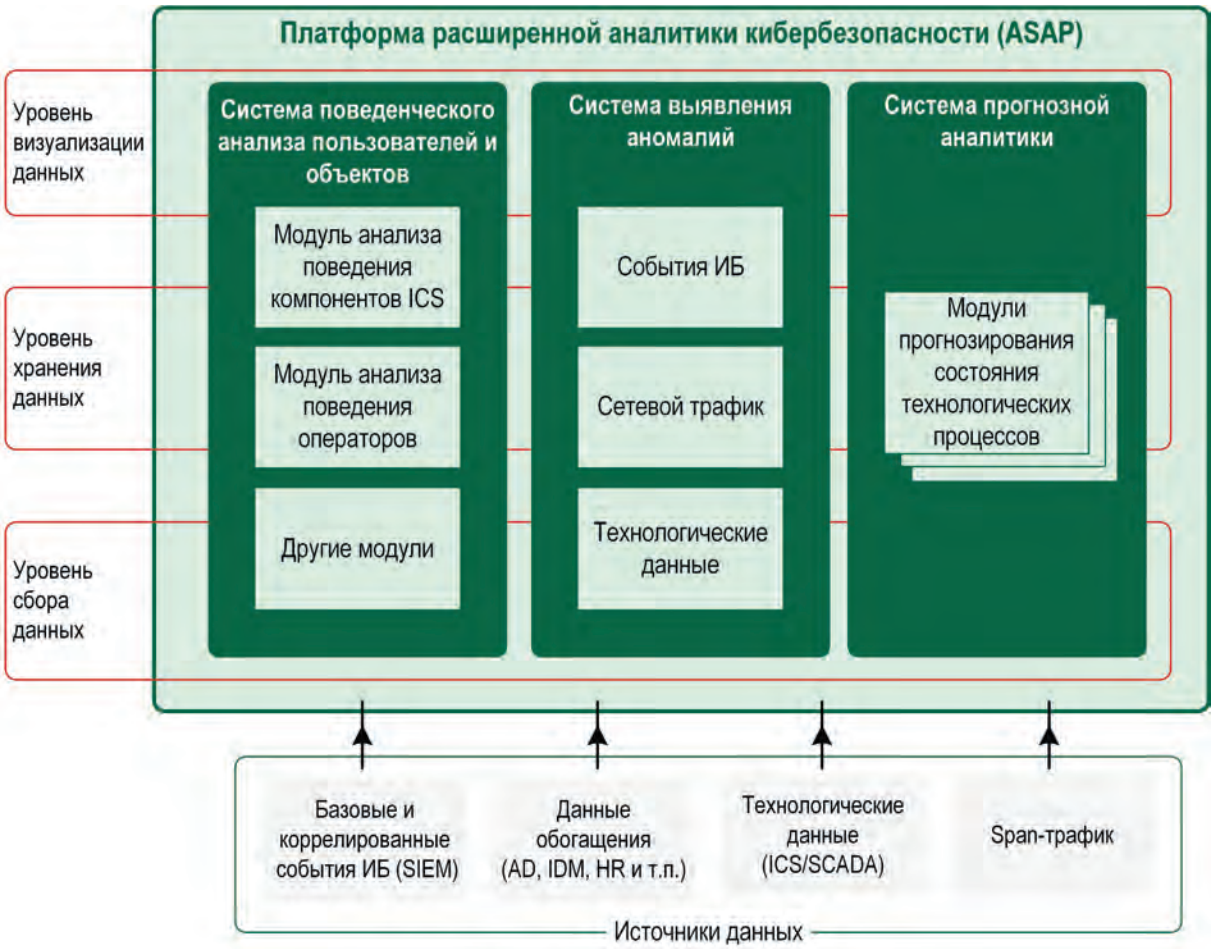

Рис. 3. Функциональные уровни ASAP

При разработке архитектуры и технологического стека платформы особое внимание уделялось возможности масштабирования (в плане производительности) и реконфигурирования модулей под разные решаемые задачи. Стек технологий ориентирован на среду Linux. Инфраструктурные технологии основаны на архитектуре микросервисов (Docker, Kubernetes), очередях сообщений (Kafka), open source продуктов хранения данных (MongoDB, PostgreSQL) и пользовательского интер-

комплексная аналитика и инструменты расширенной аналитики наиболее востребованы.

4. Промышленному характеру использования АС должны соответствовать зрелые программные продукты расширенной аналитики, разработанные на платформенных принципах и основанные на современных стеках технологий обработки больших данных.

Литература

1. Craig Rieger, Milos Manic. On Critical Infrastructures, Their Security and Resilience - Trends and Vision. arXiv: 1812.02710v1 [cs.CR]. 2018. URL: https://arxiv.org/ftp/arxiv/papers/1812/1812.02710.pdf.
2. Андерсон, Карл. Аналитическая культура. От сбора данных до бизнес результатов. М.: Манн, Иванов и Фербер, 2017. 330 с.
3. Ackerman, Pascal. Industrial Cybersecurity: Efficiently secure critical infrastructure systems. Packt Publishing. 2017. P. 456.
4. Stephen McLaughlin, Charalambos Konstantinou, Xueyang Wang, Lucas Davi, Ahmad-Reza Sadeghi, Michail Maniatakos, Ramesh Karri. The Cybersecurity Landscape in Industrial Control Systems // Proceedings of the IEEE, 2016. Vol. 104. P. 1039-1057. DOI:10.1109/JPROC.2015.2512235.
5. Зегжда, Д.П. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации / Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. // Вопросы кибербезопасности №2(26). 2018. С. 2–15.
6. Котенко, И.В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров / Котенко И.В., Левшун Д.С., Чечулин А.А., Ушаков И.А., Красов А.В. // Вопросы кибербезопасности №3(27). 2018. С. 29–38.
7. Чернов Д.В., Сычугов А.А. Современные подходы к обеспечению информационной безопасности АСУ ТП // Известия Тульского государственного университета. Технические науки. 2018. Вып. 10. С. 58-64.
8. Raihan Ul.I., Hossain M.S., Andersson K. A novel anomaly detection algorithm for sensor data under uncertainty // Soft Computing. A Fusion of Foundations, Methodologies and Applications. Soft Comput (2016). URL: https://link.springer.com/article/10.1007/s00500-016-2425-2.
9. Martí L., Sanchez-Pi N., Molina J.M., Bicharra Garcia A.C., Anomaly Detection Based on Sensor Data in Petroleum Industry Applications // Sensors 2015, 15(2), 2774-2797. URL: http://www.mdpi.com/1424-8220/15/2/.
10. Mehrotra, Kishan G., Mohan, Chilukuri, Huang, Huaming. Anomaly Detection Principles and Algorithms. Springer International Publishing 2017. P. 217.
11. Краевски Д., Ситуационное восприятие. Новый подход к дизайну человеко-машинных интерфейсов. URL: https://www.wonderware.ru/pdf/Wonderware_WhitePaper_TheNextLeapInHMI-SituationalAwareness_ru_0314.pdf.
12. Матвеев, Алексей. Обзор рынка систем поведенческого анализа – User and Entity Behavioral Analytics (UBA/UEBA). URL: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba.
13. Gorka Sadowski, Avivah Litan, Toby Bussa, Tricia Phillips. Market Guide for User and Entity Behavior Analytics. Published: 23 April 2018. ID: G00349450, Gartner, 2018.
14. Kelly Kavanagh, Gorka Sadowski, Toby Bussa. Magic Quadrant for Security Information and Event Management. Published: 3 December 2018. ID: G00348811, Gartner, 2018.
15. Уткин Л.В., Жук Ю.А. Робастная модель обнаружения аномалий с использованием модели засорения // Вестник компьютерных и информационных технологий. №7, С. 47-51, 2013.
16. Utkin L.V. A framework for imprecise robust one-class classification models // International Journal of Machine Learning and Cybernetics. 2014. Vol.5(3). P. 379-393.
17. Filonov, P., Lavrentyev, A., Vorontsov, A.:Multivariate Industrial Time Series with Cyber-Attack Simulation: Fault Detection Using an LSTM-based Predictive Data Model. 2016. URL: https://arxiv.org/abs/1612.06676.
18. Дьяконов А.Г., Головина А.М. Выявление аномалий в работе механизмов методами машинного обучения // Труды XIX Международной конференции «Аналитика и управление данными в областях с интенсивным использованием данных» (DAMDID/RCDL*2017). 2017. С.469–476.
19. Rita Sallam , James Richardson , Cindi Howson , Austin Kronz. Magic Quadrant for Analytics and Business Intelligence Platforms. Published: 11 February 2019. ID: G00354763, Gartner, 2019.
20. Peter Krensky , Erick Brethenoux , Carlie Idoine , Jim Hare , Svetlana Sicular , Shubhangi Vashisth. Magic Quadrant for Data Science and Machine-Learning Platforms. Published: 22 February 2018. ID: G00326456, Gartner, 2018.

PROBLEM ISSUES OF THE APPLICATION OF SECURITY ANALYTICAL MEANS OF CYBER-PHYSICAL SYSTEMS OF FEC ENTERPRISES

Nashivochnikov N.[7], Bolshakov A.[8], Nikolashin Yu.[9], Lukashin A.[10]

The article discusses the use of data analysis methods and technologies to ensure the security of cyber-physical systems at enterprises of the fuel and energy complex. Identified the distinctive features and highlighted the key areas of application of analytical tools of the system of operational monitoring and security analysis of cyber-physical systems of critical information infrastructure. Problem questions are formulated, the possibilities and limitations of advanced analytics tools in solving the tasks of ensuring the security of cyber-physical systems at the enterprises of the fuel and energy complex are defined. Architectural solutions of the advanced cybersecurity analytics platform are described. The presented results are based on the analysis of information from open sources: materials of scientific-practical conferences, analytical and technical reviews on the subject of security of industrial systems, and generalization of practical experience in the development, implementation, and support of integrated security systems at enterprises of the fuel and energy complex.

Keywords: *data analysis practices, anomaly detection, SIEM, advanced analytics platform, machine learning, import substitution, operational monitoring and analysis system.*

References

1. Craig Rieger, Milos Manic. On Critical Infrastructures, Their Security and Resilience - Trends and Vision arXiv: 1812.02710v1 [cs.CR]. URL: https://arxiv.org/ftp/arxiv/papers/1812/1812.02710.pdf.
2. Anderson, Karl. Analiticheskaja kul'tura. Ot sbora dannyh do biznes rezul'tatov M.: Mann, Ivanov i Ferber, 2017. 330 s.
3. Ackerman, Pascal. Industrial Cybersecurity: Efficiently secure critical infrastructure systems. Packt Publishing. 2017. P. 456.
4. Stephen McLaughlin, Charalambos Konstantinou, Xueyang Wang, Lucas Davi, Ahmad-Reza Sadeghi, Michail Maniatakos, Ramesh Karri. The Cybersecurity Landscape in Industrial Control Systems // Proceedings of the IEEE, 2016. Vol. 104. P. 1039-1057. DOI:10.1109/JPROC.2015.2512235.
5. Zegzhda, D.P. Kiberbezopasnost' progressivnyh proizvodstvennyh tekhnologij v epohu cifrovoj transformacii / Zegzhda D.P., Vasil'ev YU.S., Poltavceva M.A., Kefeli I.F., Borovkov A.I. // Voprosy kiberbezopasnosti №2(26). 2018. S. 2–15.
6. Kotenko, I.V. Kompleksnyj podhod k obespecheniyu bezopasnosti kiberfizicheskih sistem na osnove mikrokontrollerov / Kotenko I.V., Levshun D.S., CHechulin A.A., Ushakov I.A., Krasov A.V. // Voprosy kiberbezopasnosti №3(27). 2018. S. 29–38.
7. CHernov D.V., Sychugov A.A. Sovremennye podhody k obespecheniyu informacionnoj bezopasnosti ASU TP // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2018. Vyp. 10. S. 58-64.
8. Raihan Ul.I., Hossain M.S., Andersson K. A novel anomaly detection algorithm for sensor data under uncertainty // Soft Computing. A Fusion of Foundations, Methodologies and Applications. Soft Comput (2016). URL: https://link.springer.com/article/10.1007/s00500-016-2425-2.
9. Martí L., Sanchez-Pi N., Molina J.M., Bicharra Garcia A.C., Anomaly Detection Based on Sensor Data in Petroleum Industry Applications // Sensors 2015, 15(2), 2774-2797. URL: http://www.mdpi.com/1424-8220/15/2/.
10. Mehrotra, Kishan G., Mohan, Chilukuri, Huang, Huaming. Anomaly Detection Principles and Algorithms. Springer International Publishing 2017. P. 217.
11. Kraevski D., Situacionnoe vospriyatie. Novyj podhod k dizajnu cheloveko mashinnyh interfejsov. . – URL: https://www.wonderware.ru/pdf/Wonderware_WhitePaper_TheNextLeapInHMI-SituationalAwareness_ru_0314.pdf.
12. Matveev, Aleksej. Obzor rynka sistem povedencheskogo analiza– User and Entity Behavioral Analytics (UBA/UEBA). URL: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba.
13. Gorka Sadowski, Avivah Litan, Toby Bussa, Tricia Phillips. Market Guide for User and Entity Behavior Analytics. Published: 23 April 2018. ID: G00349450, Gartner, 2018.
14. Kelly Kavanagh , Gorka Sadowski , Toby Bussa. Magic Quadrant for Security Information and Event Management. Published: 3 December 2018. ID: G00348811, Gartner, 2018.
15. Utkin L.V., Zhuk Ju.A. Robastnaja model' obnaruzhenija anomalij s ispol'zovaniem modeli zasorenija // Vestnik komp'juternyh i informacionnyh tehnologij. №7, S. 47-51, 2013.

7 Nikolay Nashivochnikov, Deputy General Director - Technical Director, CISSP, Gazinformservice LLC, St.Petersburg, Russia. E-mail: cto@gaz-is.ru

8 Anatoly Bolshakov, Ph.D, Head of Analysis Technologies Department, Gazinformservice LLC, St.Petersburg, Russia. E-mail: bolshakov-a@gaz-is.ru

9 Yuri Nikolashin, Head of Development, Department of Analysis Technologies, Gazinformservice LLC, St.Petersburg, Russia. E-mail: nikolashin-y@gaz-is.ru

10 Alexey Lukashin, Ph.D, Associate Professor at the Department of Telematics (at the Central Research Institute of Robotics and Technical Cybernetics), Peter the Great St. Petersburg Polytechnic University, St.Petersburg, Russia. E-mail: alexey.lukashin@spbstu.ru

16. Utkin L.V. A framework for imprecise robust one-class classification models // International Journal of Machine Learning and Cybernetics. 2014. Vol.5(3). P. 379-393.
17. Filonov, P., Lavrentyev, A., Vorontsov, A.:Multivariate Industrial Time Series with Cyber-Attack Simulation: Fault Detection Using an LSTM-based Predictive Data Model. 2016. URL: https://arxiv.org/abs/1612.06676
18. D'yakonov A.G., Golovina A.M. Vyyavlenie anomalij v rabote mekhanizmov metodami mashinnogo obucheniya // Trudy XIX Mezhdunarodnoj konferencii «Analitika i upravlenie dannymi v oblastyah s intensivnym ispol'zovaniem dannyh» (DAMDID/RCDL*2017). 2017. S.469–476.
19. Rita Sallam , James Richardson , Cindi Howson , Austin Kronz. Magic Quadrant for Analytics and Business Intelligence Platforms. Published: 11 February 2019. ID: G00354763, Gartner, 2019.
20. Peter Krensky , Erick Brethenoux , Carlie Idoine , Jim Hare , Svetlana Sicular , Shubhangi Vashisth. Magic Quadrant for Data Science and Machine-Learning Platforms. Published: 22 February 2018. ID: G00326456, Gartner, 2018.