АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

УДК 004.056.5

Вестник УрФО № 1(39) / 2021, с. 43–53

Абдулин А. А., Соколов А. Н.

DOI: 10.14529/secur210106

ИССЛЕДОВАНИЕ ПРОГРАММНЫХ РЕШЕНИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СЕТЕЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ[1]

В статье представлены исследования современных программных решений обеспечения информационной безопасности промышленных сетей. Функциональные возможности выбранных продуктов классифицированы в соответствии с требованиями архитектуры адаптивной безопасности: обнаружение угроз, реагирование на инциденты, прогнозирование возникновения инцидентов, предотвращение возникающих угроз. Проведен сравнительный анализ выбранных систем обеспечения информационной безопасности промышленных сетей. Выделены универсальные программные решения обеспечения информационной безопасности промышленных сетей, а так программные продукты, наиболее подходящие для тех или иных направлений обеспечения информационной безопасности.

Ключевые слова: *Автоматизированная система управления технологическим процессом, система контроля уязвимостей, SCADA-система, оркестровка безопасности, система обнаружения угроз.*

[1] Исследование выполнено при финансовой поддержке гранта РФФИ и Челябинской области в рамках научного проекта № 20-47-740006

RESEARCH OF SOFTWARE SOLUTIONS FOR PROVIDING INFORMATION SECURITY OF INDUSTRIAL NETWORKS OF AUTOMATED PROCESS CONTROL SYSTEMS

The article presents studies of modern software solutions for information security of industrial networks. The functionality of the selected products is classified according to the requirements of the adaptive security architecture: threat detection, incident response, incident prediction, prevention of emerging threats. A comparative analysis of the selected information security systems for industrial networks was carried out. The universal software solutions of information security of industrial networks are distinguished, and also the software products which are the most suitable for these or those directions of information security.

Keywords: *Automated process control system, vulnerability control system, SCADA system, security orchestration, threat detection system.*

С началом периода внедрения вычислительной техники в системы управления связано появление термина «автоматизированная система управления» (АСУ). Будучи задействованными в критической инфраструктуре промышленных сетей, автоматизированные системы управления технологическими процессами (АСУ ТП) строятся на основе отказоустойчивой, высоконадежной вычислительной техники. Это техника промышленного исполнения, созданная специально для долговременной, круглосуточной эксплуатации на индустриальных объектах. Последствия сбоя или отказа работы систем представляет серьезную угрозу для оборудования, а также для жизни и здоровья людей.

АСУ ТП имеет стандартную трехзвенную структуру, и какой бы ни была ее отказоустойчивость, средний её уровень — SCADA-системы, — является наиболее уязвимым, и позволяет злоумышленнику производить ряд манипуляций с технологическим процессом, в том числе вопреки отказоустойчивости.

Безопасность АСУ ТП – это практика защиты сетей диспетчерского управления и сбора данных (SCADA), общей структуры систем управления, используемых в промышленных операциях. Эти сети отвечают за автоматическое, дистанционное управление необходимыми товарами и услугами, такими как вода, природный газ, электричество и транспорт для миллионов людей. SCADA является одним из наиболее распространенных типов систем управления производством (ICS).

Эти сети, как и любая другая сеть, находятся под угрозой кибератак, которые могут быстро и с тяжелыми последствиями разрушить любую часть критической инфраструктуры, если не будет обеспечена надлежащая безопасность. Капитальные затраты – еще одна ключевая проблема: системы SCADA могут стоить организации от десятков тысяч до миллионов долларов. По этим причинам важно, чтобы организации внедряли надежные меры безопасности SCADA для защиты своей инфраструктуры, которые могут потенциально пострадать от сбоев, вызванных внешней атакой или внутренней ошибкой [1, с. 4].

За последние годы подходы к обеспечению безопасности АСУ ТП значительно изменились. До появления компьютеров единственным способом мониторинга сети SCADA была группа из нескольких человек на каждой станции для подготовки отчетности о состоянии каждой системы. На более загруженных станциях постоянно работали технические специалисты для ручного управления сетью и связи по телефонным линиям.

Только после появления локальных сетей (LAN) и достижений в направлении миниатюризации систем, стали видимыми достижения в развитии АСУ ТП, такие как, например, распределенная сеть SCADA. Позже появились сетевые системы, которые смогли обмениваться данными через глобальную сеть (WAN) и соединять вместе множество других компонентов.

Начиная с местных компаний и заканчивая федеральными правительствами, каждая организация, которая работает с системами SCADA, уязвима. Эти угрозы могут иметь далеко идущие последствия, как для экономики, так и для общества. Угрозы для сетей SCADA можно разбить на несколько групп:

• **Хакеры** – отдельные лица или группы лиц со злым умыслом. Получив доступ к ключевым компонентам SCADA, хакеры могут развязать хаос в организации, который может варьироваться от перебоев в обслуживании до кибервойны.

• **Malware** – вредоносное ПО, включая вирусы, шпионское и вымогательское ПО, которое представляет опасность для систем SCADA. Несмотря на то, что вредоносное ПО может специально не предназначаться для самой сети, оно все же может представлять угрозу для ключевой инфраструктуры, которая помогает управлять сетью SCADA. Это включает в себя мобильные приложения, которые используются для мониторинга и управления системами SCADA.

• **Террористы** – в отличие от «хакеров», целью которых является получение денег, руководствуются стремлением создать хаос и причинить как можно ущерба.

• **Сотрудники** – могут создавать внутренние угрозы, которые могут быть не менее разрушительными, чем внешние (от ошибки, связанной с человеческим фактором, до недовольного сотрудника или подрядчика). Важно, чтобы безопасность SCADA устраняла эти риски.

Управление современными сетями SCADA без принятия надлежащих мер безопасности может создавать серьезные риски. Многие сети по-прежнему не имеют необходимых систем обнаружения и мониторинга, и это делает их уязвимыми для атак. Поскольку сетевые атаки SCADA используют как киберфизические, так и физические уязвимости, необходимо соответствующим образом согласовать меры кибербезопасности [2].

Системы контроля уязвимостей — один из эффективных методов противодействия промышленным киберугрозам. Это узкопрофильные программы, разработанные специально для промышленных систем автоматизации. Они позволяют определить целостность внутренней среды устройства, зафиксировать все попытки изменить прикладную программу контроллера, изменения в конфигурации сетевых устройств защиты и управления в энергосетях.

В ходе исследования были выбраны ключевые пункты, представленные в таблице 1, такие как:

1) обнаружение угроз нулевого дня, уязвимость нулевого дня;

2) возможность интеграции с центром обеспечения безопасности, с системами управления информационной безопасностью;

3) анализ и обнаружение аномалий сетевого трафика;

4) возможность инвентаризации устройств;

5) оркестровка безопасности — это стек решений программ, собирающий данные об угрозах безопасности из нескольких источников и реагировать на события безопасности низкого уровня без помощи человека;

6) наличие функции пассивного мониторинга сети;

7) формирование журналов учета событий;

8) отображение топологии сети и возможность ее сегментации;

9) возможность мультиместного и безагентонго развёртывания и т.д.

Исследование представленных программных решений позволило сделать следующие выводы.

Nozomi Networks предлагает единое решение для контроля рисков в режиме реального времени. Высокая точность и минимальность ложных срабатываний достигается за счет инновационного использования искусственного интеллекта и машинного обуче-

Таблица 1

Программные решения обеспечения информационной безопасности промышленных сетей

Возможности	NOZOMI (NG)	CLAROTY	CYBERX Platform	DRAGOS ICP	Forescout PLATFORM	INDEGY ICS	Kaspersky (KICS)
1. Обнаружение угроз							
Обнаружение аномалий	Yes	Yes	Yes	Yes			Yes
Автоматическое обнаружение активов	Yes		Yes	Yes	Yes	Yes	
Обнаружение потока				Yes			Yes
Обнаружение PLC- и RTU-устройств			Yes	Yes		Yes	Yes
Отображение топологии сети	Yes	Yes	Yes	Yes		Yes	Yes
Инвентаризация устройств	Yes	Yes	Yes	Yes		Yes	
Фильтры просмотра	Yes	Yes	Yes	Yes		Yes	Yes
Обнаружение мошеннических устройств	Yes		Yes		Yes	Yes	Yes
Обнаружение угроз нулевого дня	Yes		Yes			Yes	Yes
Обнаружение угроз с контекстом	Yes	Yes	Yes	Yes	Yes		
ICS анализ угроз			Yes	Yes		Yes	Yes
Глубокий анализ пакетов (DPI)			Yes	Yes	Yes	Yes	Yes
Сегментация сети	Yes				Yes		
Зеркалирование портов			Yes	Yes		Yes	Yes
2. Реагирование на инциденты							
Смягчение событий безопасности	Yes			Yes	Yes	Yes	
Оповещения Data Historian	Yes		Yes	Yes		Yes	
Контроль приложений	Yes	Yes		Yes	Yes	Yes	Yes
3. Прогнозирование возникновения инцидентов							
Анализ трафика	Yes		Yes	Yes		Yes	Yes
Оркестровка безопасности			Yes	Yes	Yes	Yes	
Мониторинг изменений	Yes	Yes		Yes		Yes	

Продолжение таблицы 1

Отчет об оценке уязвимости	Yes		Yes	Yes	Yes	Yes	Yes
Постоянный мониторинг		Yes	Yes			Yes	Yes
Журнал событий		Yes				Yes	Yes
4. Предотвращение угроз							
Смягчение событий безопасности	Yes			Yes	Yes	Yes	
Оповещения Data Historian	Yes		Yes	Yes		Yes	Yes
Контроль периметра	Yes	Yes		Yes	Yes	Yes	Yes

ния. Интегрированная инфраструктура безопасности включает встроенные интеграции для систем управления активами и идентификацией, SIEM [3].

Основные функциональные возможности системы Nozomi Networks (рис. 1):

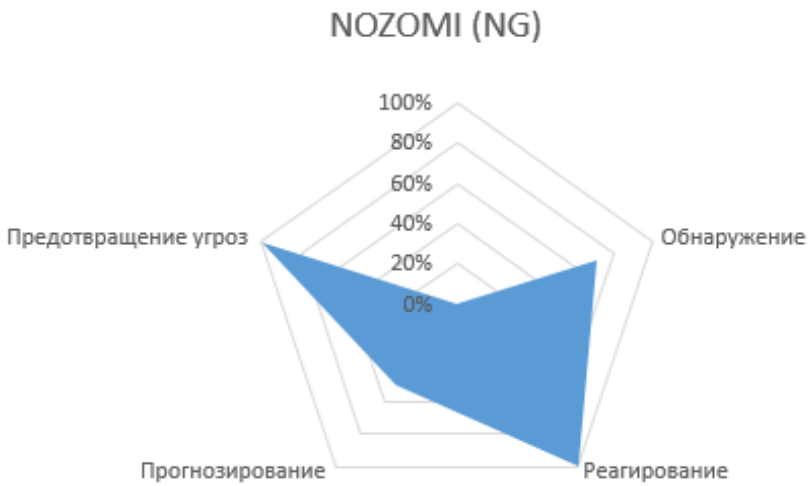

Рис. 1. Функциональные возможности NOZOMI (NG)

1. Обнаружение:
• обнаружение аномалий на основе поведения;
• правила и сигнатурное обнаружение;
• продвинутая корреляция для детального понимания и быстрое восстановление;
• OT ThreatFeed для существующих угроз и уязвимостей.
2. Реагирование:
• автоматический захват пакета;
• снимки системы TimeMachine.
3. Прогнозирование:
• мониторинг изменений;
• отчет об оценке уязвимости.
4. Предотвращение угроз:
• смягчение событий безопасности;
• оповещения Data Historian;
• контроль периметра.

Claroty Platform предоставляет группам безопасности исключительную видимость в промышленных сетях управления и мониторинг в режиме реального времени. Мониторинг способен распознать продвинутые угрозы и вовремя выявить уязвимости сети. Платформа позволяет сегментировать сеть, контролировать и предоставлять безопасный удаленный доступ, составлять детализированные политики доступа и записывать сеансы [4].

Основные функциональные возможности системы Claroty Platform (рис. 2):

1. Обнаружение:
• постоянный мониторинг (обнаружение угроз с контекстом, мониторинг изменений);
• обнаружение вредоносной активности и рискованных изменений в течение всей атаки «kill-chain».

2. Реагирование:

• контекстные оповещения для быстрой сортировки и расследования;

• формирование автоматизированного ответа на основе существующей сетевой инфраструктуры.

3. Прогнозирование:

• превентивно выявляет и устраняет уязвимости, неверные конфигурации и незащищенные соединения.

4. Предотвращение угроз:

• точные периодические запросы активов ОТ и ИТ;

• безопасный запрос ресурсов ICS и не-ICS для улучшения видимости конфигураций активов;

• расширенный контекст для предупреждений и уязвимостей.

Платформа **CyberX** обеспечивает непрерывный мониторинг угроз ICS и обнаружение активов, объединяя глубокое понимание промышленных протоколов, устройств и приложений с определением поведенческих аномалий, специфичным для ICS, анализом угроз, анализом рисков и автоматизированным моделированием угроз.

Безагентная платформа безопасности CyberX ОТ позволяет клиентам автоматически обнаруживать ИТ-активы, видеть топологию сети, выявлять критические уязвимости и векторы атак. Решение дает возможность постоянно отслеживать ОТ сети на предмет разрушительных кибератак [5].

Основные возможности системы CYBERX Platform (рис. 3):

1. Обнаружение:

• непрерывный мониторинг;

• поведенческая аналитика с самообучением;

• запатентованные алгоритмы с поддержкой ICS.

2. Реагирование:

• возможности глубокой криминалистической экспертизы, расследования и поиска угроз;

• полноценные PCAP для анализа детализации;

• встроенная интеграция на уровне приложений с IBM QRadar, Splunk и ServiceNow.

3. Прогнозирование:

• автоматизированное моделирование угроз для прогнозирования наиболее вероятных путей векторов атак;

• определение базовых моделей поведения и конфигураций;

• собственный специфический для ICS анализ угроз (нулевые дни, вредоносные программы, злоумышленники).

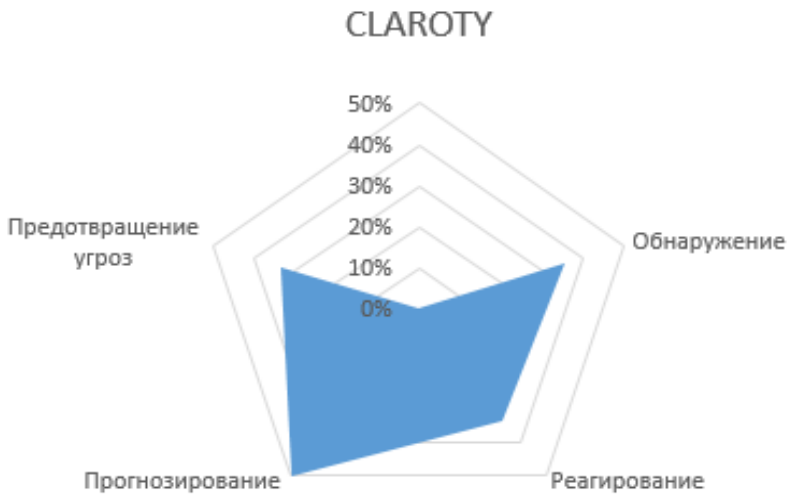

Рис. 2. Функциональные возможности CLAROTY Platform

4. Предотвращение угроз:

• запатентованные оценки рисков и уязвимостей, характерные для ICS, включая обнаружение активов;

• упреждающая, основанная на оценке риска приоритизация действий по смягчению последствий для защиты критических активов;

• интеграция с ведущими технологиями предотвращения, включая межсетевые экраны следующего поколения, однонаправленные шлюзы и безопасный удаленный доступ, защита привилегированных учетных записей.

Dragos Industrial Cybersecurity Platform — это защитное решение для промышленных сетей, которое автоматически находит и идентифицирует активы сети. Программа сканирует активы, находя неправильные настройки, возможности улучшения конфигурации. В случае выявления подозрительной активности, платформа предоставляет пошаговое руководство к расследованию и реагированию на инцидент и инструменты для устранения неполадок [6].

Forescout Platform — единая платформа, позволяющая применять адаптивные, детализированные политики и быстро просматривать результаты, используя существующую физическую и виртуальную сетевую инфраструктуру [7]. Основные функциональные возможности Forescout Platform (рис. 5):

1. Обнаружение:
- автоматическое обнаружение активов;
- обнаружение мошеннических устройств;
- обнаружение угроз с контекстом;

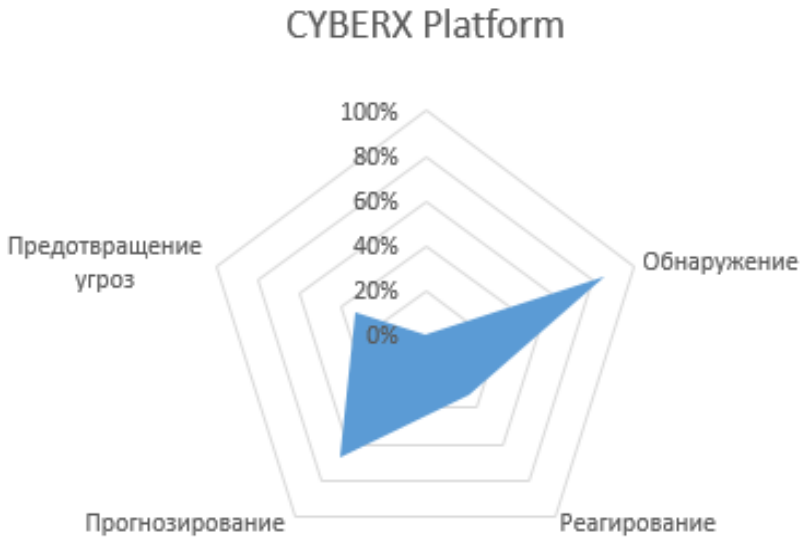

Рис. 3. Функциональные возможности CYBERX Platform

Основные возможности системы Dragos Industrial Cybersecurity Platform (рис. 4):

1. Обнаружение:

Сложные характеристики тактик, методов и процедур противника с помощью анализа поведения угроз выявляют злонамеренную активность в сетях ICS и предоставляют подробный контекст для предупреждений.

2. Реагирование:
- смягчение событий безопасности;
- оповещения Data Historian;
- контроль приложений.

3. Прогнозирование:

Глубокая проверка пакетов (DPI) протоколов ICS, характеристик трафика и активов, возможность использования журналов узлов и событий контроллера, а также интеграция с активами ICS, такими как исторические данные, обеспечивают полное представление о средах ICS.

4. Предотвращение угроз:
- смягчение событий безопасности;
- оповещения Data Historian;
- контроль периметра.
- глубокий анализ пакетов (DPI);
- зеркалирование портов.

2. Реагирование:
- смягчение событий безопасности;
- контроль периметра.

3. Прогнозирование:
- оркестровка безопасности;
- отчет об оценке уязвимости.

4. Предотвращение угроз:
- смягчение событий безопасности;
- контроль периметра.

Indegy Industrial Cybersecurity Suit обеспечивает отслеживание активов, обнаружение и смягчение угроз, управление уязвимостями и обеспечение целостности устройства. Она способна защитить сеть не только от зловредного вмешательства, но и от непреднамеренных человеческих ошибок [8].

Основные возможности Indegy Industrial Cybersecurity Suit (рис. 6):

1. Обнаружение:
- автоматическое обнаружение пакетов;
- пассивный мониторинг сети.

2. Реагирование:

Рис. 4. Функциональные возможности DRAGOS ICP

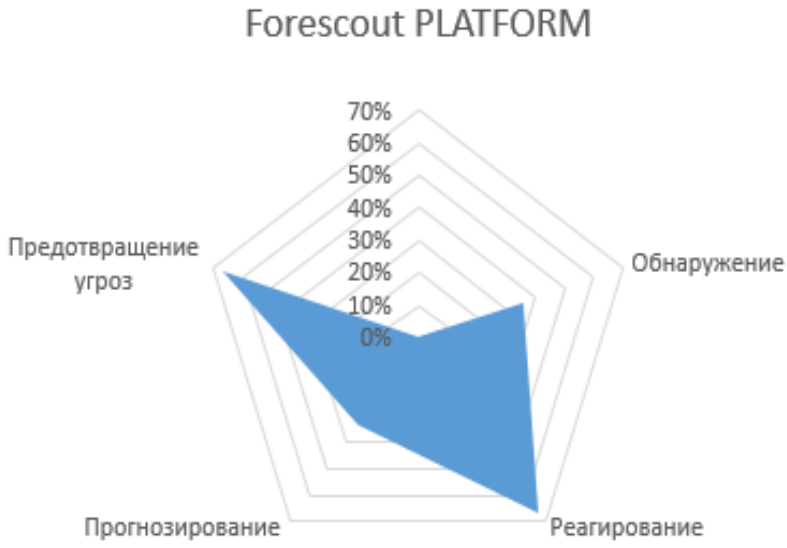

Рис. 5. Функциональные возможности Forescout Platform

• смягчение событий безопасности;
• оповещения Data Historian;
• контроль периметра.
3. Прогнозирование:
• анализ трафика;
• оркестровка безопасности;
• мониторинг изменений;
• отчет об оценке уязвимости;
• постоянный мониторинг;
• журнал событий.
4. Предотвращение угроз.

Kaspersky Industrial CyberSecurity – это набор технологий и сервисов, призванный защитить промышленные системы всех уровней (включая серверы SCADA, панели HMI, инженерные рабочие станции, ПЛК, сетевые соединения и персональное оборудование), сохраняя при этом стабильность и непрерывность технологических процессов. Каждая промышленная среда уникальна, поэтому решение адаптируемо под конкретную отрасль – например, нефтегазовый сектор, энергетические сети, производство. При этом решение не влияет на непрерывность технологических процессов [9].

Основные возможности Kaspersky Industrial CyberSecurity (рис. 7).

1. Обнаружение:
• обнаружение аномалий;
• обнаружение потока;
• обнаружение PLC- и RTU-устройств;
• отображение топологии сети;

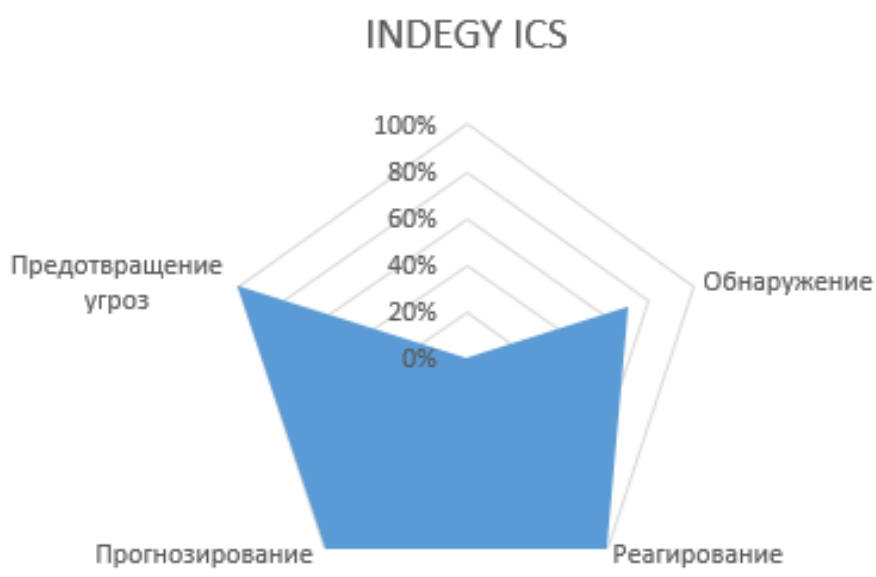

Рис. 6. Функциональные возможности INDEGY ICS

Рис. 7. Функциональные возможности Kaspersky (KICS)

- инвентаризация устройств;
- фильтры просмотра;
- обнаружение мошеннических устройств;
- обнаружение угроз нулевого дня;
- ICS анализ угроз;
- глубокий анализ пакетов (DPI);
- сегментация сети;
- зеркалирование портов.

2. Реагирование:
- контроль приложений.

3. Прогнозирование:
- анализ трафика;
- оркестровка безопасности;
- мониторинг изменений;
- отчет об оценке уязвимости;
- постоянный мониторинг;
- журнал событий.

4. Предотвращение угроз:
- оповещения Data Historian;
- контроль периметра.

На основе проведенных исследований можно сделать вывод, что наиболее полным функционалом для обеспечения всех четырех требований архитектуры адаптивной безопасности, обладают продукты DRAGOS ICP и INDEGY ICS.

Полученные результаты позволяют выбрать подходящие решения для конкретной

ситуации. Если, например, необходима система только для обнаружения угроз, наиболее подходящим вариантом является CYBERX Platform, которая обладает возможностями автоматического обнаружения устройств, топологии сети, аномалий, мошеннических устройств и т.д.

NOZOMI (NG) и Forescout Platform специализируются на предотвращении и реагировании на возникающие угрозы. Эти программные продукты имеют возможности контроля периметра и приложения, а так же систему оповещения Data Historian, что позволяет наиболее эффективно бороться с возникающими угрозами.

Kaspersky Industrial CyberSecurity имеет наиболее полный функционал в области обнаружения, предотвращения и прогнозирования угроз. Для эффективного прогнозирования будущих угроз, Kaspersky Industrial CyberSecurity имеет систему постоянного мониторинга трафика, его глубокого анализа, обнаружение аномалий.

Литература

1. Абдулин А.А. Методы оценки уязвимостей автоматизированных систем управления технологическими процессами /Абдулин А.А., Соколов А.Н. //Сборник трудов XVII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства», г. Челябинск, 2018, с 4 – 9.

2. Кибербезопасность АСУ ТП. Обзор специализированных наложенных средств защиты [Электронный ресурс] – https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review (дата обращения: 03.11.2020).

3. Industrial Strength OT and IoT Security and Visibility [Электронный ресурс] – https://www.nozominetworks.com/downloads/US/Nozomi-Networks-Guardian-Data-Sheet.pdf (дата обращения: 19.11.2020).

4. Continuous Threat Detection [Электронный ресурс] – https://cdn2.hubspot.net/hubfs/2553528/CTDdatasheet.pdf (дата обращения: 14.01.2021).

5. Learn why industrial control systems are soft targets for adversaries [Электронный ресурс] – https://cyberx-labs.com/resources/risk-report-2019/ (дата обращения: 03.02.2021).

6. Industrial Control Threat Intelligence Whitepaper [Электронный ресурс] – https://www.dragos.com/resource/industrial-control-threat-intelligence-whitepaper/ (дата обращения: 15.12.2020).

7. The Forescout Platform Complete Situational Awareness for the Extended Enterprise [Электронный ресурс] – https://www.forescout.com/platform/ (дата обращения: 01.12.2020).

8. The Indegy IndustrialCybersecurity Suite [Электронный ресурс] – https://cdn2.hubspot.net/hubfs/2755567/The%20Indegy%20Industrial%20Cybersecurity%20eBook%202019.pdf (дата обращения: 11.02.2021).

9. Kaspersky Industrial CyberSecurity [Электронный ресурс] –www.dialognauka.ru URL: https://www.dialognauka.ru/products/KICS/ (дата обращения: 10.11.2020).

References

1. Abdulin A.A., Methods of vulnerability assessment of automated control systems of technological processes / A.A. Abdulin, A.N. Sokolov // Proceedings of the XVII All-Russian scientific-practical conference of students, graduate students and young scientists "Security of Information Space", Chelyabinsk 2018, pp. 4-9.

2. Cybersecurity of APCS. Review of specialized superimposed protection tools [Electronic resource] - https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review (date of reference: 03.11.2020).

3. Industrial Strength OT and IoT Security and Visibility [Electronic resource] - https://www.nozominetworks.com/downloads/US/Nozomi-Networks-Guardian-Data-Sheet.pdf (accessed 19.11.2020).

4. Continuous Threat Detection [Electronic resource] - https://cdn2.hubspot.net/hubfs/2553528/CTDdatasheet.pdf (accessed 14.01.2021).

5. Learn why industrial control systems are soft targets for adversaries [Electronic resource] - https://cyberx-labs.com/resources/risk-report-2019/ (accessed 03.02.2021).

6. Industrial Control Threat Intelligence Whitepaper [Electronic resource] - https://www.dragos.com/resource/industrial-control-threat-intelligence-whitepaper/ (accessed 15.12.2020).

7. The Forescout Platform Complete Situational Awareness for the Extended Enterprise [Electronic resource] - https://www.forescout.com/platform/ (accessed 01.12.2020).

8. The Indegy IndustrialCybersecurity Suite [Electronic resource] - https://cdn2.hubspot.net/hubfs/2755567/The%20Indegy%20Industrial%20Cybersecurity%20eBook%202019.pdf (accessed 11.02.2021).

9. Kaspersky Industrial CyberSecurity [Electronic resource] -www.dialognauka.ru URL: https://www.dialognauka.ru/products/KICS/ (access date: 10.11.2020).

АБДУЛИН Артур Ахмадулович, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: arthyrw@gmail.com

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

Abdulin Arthur Akhmadulovich, postgraduate student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: arthyrw@gmail.com

SOKOLOV Alexander Nikolaevich, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru