Надежность, том 25, №2, 2025 / Dependability 2, 2025
Защита информации

УДК 681.32
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-2-59-66

Методология глубокого анализа пакетов данных как средства обеспечения адекватности спецификаций, передаваемых в промышленных сетях

A method for deep packet inspection as means of ensuring the adequacy of specifications transmitted in industrial networks

Чаус Е.А.[1]*, Юркевич Е.В.[2]
Chaus E.A.[1]*, Yurkevich E.V.[2]

[1] *ПАО «Группа Черкизово», Российская Федерация, Москва*
[2] *ФГБУН Институт проблем управления им. В. А. Трапезникова Российской академии наук, Российская Федерация, Москва*
[1] *Cherkizovo Group, Russian Federation, Moscow*
[2] *V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Russian Federation, Moscow*
** zc86@mail.ru*

Чаус Е.А.

Юркевич Е.В.

Резюме. Цель. *Повышение адекватности спецификаций, передаваемых в системах автоматизации производственных процессов, связанных с безопасностью.* **Методы.** *Интеграция технологии глубокого контроля пакетов данных в работу открытой платформы коммуникаций с унифицированной архитектурой. Применение такой платформы в промышленных сетях определяется нормами реализации трафика сообщений в соответствии с российскими стандартами. На основании статистического анализа существующих угроз применению программных технологий использован подход, основанный на применении единого интерфейса в средствах управления объектами автоматизации технологических процессов. Применение технологии глубокой проверки сетевых пакетов по их содержимому позволило разработать алгоритм накопления статистических данных, определяющих эффективность регулирования и фильтрации трафика. На базе использования такой технологии предлагаемые методологические положения расчета рисков в работе систем автоматизации направлены на учет технических и операционных аспектов угроз влияния внешних факторов.* **Результаты.** *Показано, что соблюдение требований, предлагаемых для введения в нормативные документы, и положений, определяющих устойчивость транзакций, позволяет интернет-провайдерам визуализировать существующий трафик, определять его узкие места, вводить алгоритмизацию в использование сетевых ресурсов включая ее влияние на производительность сети и совместимость с различными протоколами. На основе результатов глубокого контроля пакетов данных рассмотрены возможности проведения эффективного анализа содержимого пакетов и их метаданных. Разработан алгоритм глубокого контроля пакетов данных, который демонстрирует этапы захвата, анализа и обработки сетевого трафика, а также структурная схема размещения средств реализации этого алгоритма в сети открытых распределенных систем, включающая точки интеграции между промышленными контроллерами, серверами и клиентами, а также облачными сервисами. Данная схема помогает визуализировать, интеграцию технологии глубокого контроля пакетов данных на все уровни взаимодействия элементов систем автоматизации производственных процессов. Для контроля динамики рисков предложен алгоритм, основанный на учете развития угроз работе каждого элемента, а также для построения контрмер в системах автоматизации производственных процессов. Характеристики средств, являющихся такими контрмерами угрозам внешних воздействий, определяются соответствием пакетов передаваемых данных нормам, определяющим спецификации протокола сервера открытой платформы. Получаемая информация помогает администраторам контролировать трафик, выявлять аномалии и планировать пропускную способность каналов связи в рассматриваемых системах автоматизации технологических процессов. Описанный подход к построению схемы обнаружения киберугроз является стратегической основой для обеспечения безопасности использования критически важных приложений.* **Заключение.** *Для обеспечения безопасности промышленных систем автоматизации технологических процессов введение норм, определяющих технологию глубокого контроля пакетов данных, в российские стандарты на цифровое производство является существенным шагом к повышению адекватности спецификаций, передаваемых в промышленных сетях, в условиях растущих киберугроз.*

Abstract. Aim. *To improve the adequacy of specifications transmitted within safety-critical process automation systems.* **Methods.** *Integration of deep packet inspection technology into the operation of an open communications platform with a uniform architecture. The application of such a platform in industrial networks is defined by the requirements of the Russian standards as regards the implementation of messaging traffic. The paper employed an approach that is based on the statistical analysis of existing threats to the use of software technologies and single interfaces as part of process automation tools. Content-based deep packet inspection allowed developing an algorithm for accumulating statistical data that define the efficiency of traffic regulation and filtering. Using the above technology along with the proposed method for calculating risks affecting automation systems would allow taking into account the technological and operational aspects of the external factors.* **Results.** *It was shown that compliance with the proposed regulatory requirements, as well as provisions defining the stability of transactions will allow Internet providers visualising existing traffic, identifying its bottlenecks, algorithmising the use of network resources, including its effect on network performance and compatibility with various protocols. Based on the results of deep packet inspection, the paper examined the feasibility of effective analysis of packet content and metadata. An algorithm was developed for deep packet inspection that demonstrates capturing, analysis, and processing of network traffic along with a diagram of the allocation of the means and facilities implementing the algorithm in a network of open distributed systems that includes integration points between industrial controllers, servers, and clients, as well as cloud services. The diagram helps visualising the integration of deep packet inspection technology at all levels of interaction between the elements of process automation systems. To control the risk dynamics, an algorithm was proposed that takes into account the evolution of threats to each of the elements, as well as building countermeasures within process automation systems. The characteristics of the facilities that represent such countermeasures to external threats are defined by the compliance of the transmitted data packets with the requirements that define the protocol specifications of an open platform server. The obtained information helps administrators inspect traffic, identify anomalies and plan the capacity of communication channels within the examined process automation systems. The above approach to building a cyber threat detection framework is a strategic basis for ensuring the security of critical applications.* **Conclusions.** *Given the demand for ensuring the safety of process automation systems, the introduction of requirements defining the deep packet inspection process into Russian digital manufacturing standards would be a significant step towards improving the adequacy of specifications transmitted within industrial networks in the face of growing cyber threats.*

Ключевые слова: *технология глубокого анализа пакетов данных, адекватность спецификаций, открытая распределенная система, промышленные сети, унифицированная архитектура, кибератаки, безопасность промышленных систем, защита данных, аутентификация, анализ пакетов.*
Keywords: *deep packet inspection process, adequacy of specifications, open distributed system, industrial networks, uniform architecture, cyber attacks, security of industrial systems, data protection, authentication, packet analysis.*

Для цитирования: *Чаус Е.А., Юркевич Е.В. Методология глубокого анализа пакетов данных как средства обеспечения адекватности спецификаций, передаваемых в промышленных сетях // Надежность. 2025. №2. С. 59-66. https://doi.org/10.21683/1729-2646-2025-25-2-59-66*
For citation: *Chaus E.A., Yurkevich E.V. Method for deep packet inspection as means of ensuring the adequacy of specifications transmitted in industrial networks. Dependability 2025;2:59-66. https://doi.org/10.21683/1729-2646-2025-25-2-59-66*

Поступила: *11.11.2024* / **После доработки:** *10.01.2025* / **К печати:** *09.06.2025*
Received on: *11.11.2024* / **Revised on:** *10.01.2025* / **For printing:** *09.06.2025*

Введение

Технология глубокой проверки пакетов данных (*Deep Packet Inspection* (*DPI*)) представляет собой важный инструмент анализа сетевого трафика, позволяющий отслеживать и фильтровать информацию об элементах рассматриваемых систем в реализации конкретного технологического процесса, а также в режиме реального времени контролировать адекватность содержимого пакетов сообщений, передаваемых между элементами системы. Данная технология обеспечивает возможность подробного анализа и мониторинга транзакций, определяющих базу для обеспечения безопасности, качества обслуживания (*QoS*) в управлении сетевым трафиком [1, 2].

В 2023 году объем мирового рынка DPI оценивался в 24,19 млрд долларов США. По прогнозам международной компании *Fortune Business Insights*, этот рынок вырастет с 30,38 млрд долларов США в 2024 году до 202,94 млрд долларов США к 2032 году, при этом среднегодовой темп роста составит 26,8% в течение прогнозируемого периода [3].

По мере развития цифровой трансформации средств связи проверка элементов сообщений, составляющая глубокий анализ содержания пакетов данных, начинает играть решающую роль в обеспечении безопасности транзакций и оптимизации сетевой среды. Сегодня *DPI* применяется в широком классе секторов систем связи, например, телекоммуникации, средства обеспечения кибербезопасности, оптимизация работы сети. Ключевые элементы таких систем включают в себя передовые аппаратные и программные решения, предназначенные для анализа сетевых пакетов в реальном масштабе времени, помогая организациям повышать безопасность и эффективность работу сети [42].

По мере увеличения сложности и масштабов промышленных систем автоматизации возрастает и уровень потенциальных угроз, делая критически важной адекватность передаваемого контента. Всемирно признанным стандартом, регламентирующим обеспечение надежной и безопасной передачи данных в системах автоматизации технологических процессов, является нормативное обеспечение открытой платформы коммуникаций с унифицированной архитектурой (*Open Platform Communications Unified Architecture* (*OPC UA*)) [5].

В ориентации на нормы *OPC UA*, применение *DPI* может значительно повысить эффективность систем защиты, предоставляя новые возможности для управления промышленными сетями. Основные положения, определяющие работу систем, связанных с безопасностью, определены в ГОСТ Р МЭК 61508. Важной характеристикой этих систем является то, что их работа сама по себе не опасна, но нештатный результат их работы может быть опасен.

На примере таких систем предлагается рассмотрение методологических положений глубокого контроля пакетов данных, направленных на обеспечение адекватности спецификаций, передаваемых в промышленных сетях.

1. Открытые распределенные системы и их применение

Внешние воздействия на системы управления производственными процессами, влияющими на способность платформы коммуникаций передавать и получать информацию, порождают неопределенности, в отношении достижимости целей, поставленных перед разработчиками систем автоматизации (АСУ). Фактически вся деятельность, связанная с эксплуатацией АСУ, содержит риски, учитывающие влияние этих неопределенностей. Ставится задача оценки рисков на каждом из этапов жизненного цикла АСУ от приемных испытаний разработки до выведения ее из эксплуатации.

Построение унифицированной архитектуры (*UA*) открытых распределенных систем (OPC), регламентируется российскими стандартами, определяющими механизмы передачи данных и взаимодействия устройств в промышленных сетях. Данные стандарты являются универсальной системой нормативных документов, регламентирующих всесторонние аспекты кроссплатформенного обмена данными в системах автоматизации производственных процессов. Нормы OPC *UA* обеспечивают высокую надежность и безопасность передачи сообщений, они ориентированы на поддержание эффективной реализации широкого класса промышленных сценариев, от операций на производственных линиях до управления энергетическими системами [4].

Структура OPC *UA* основывается на взаимодействии серверов, предоставляющими данные, и клиентов, обменивающихся данными с серверами. Применение

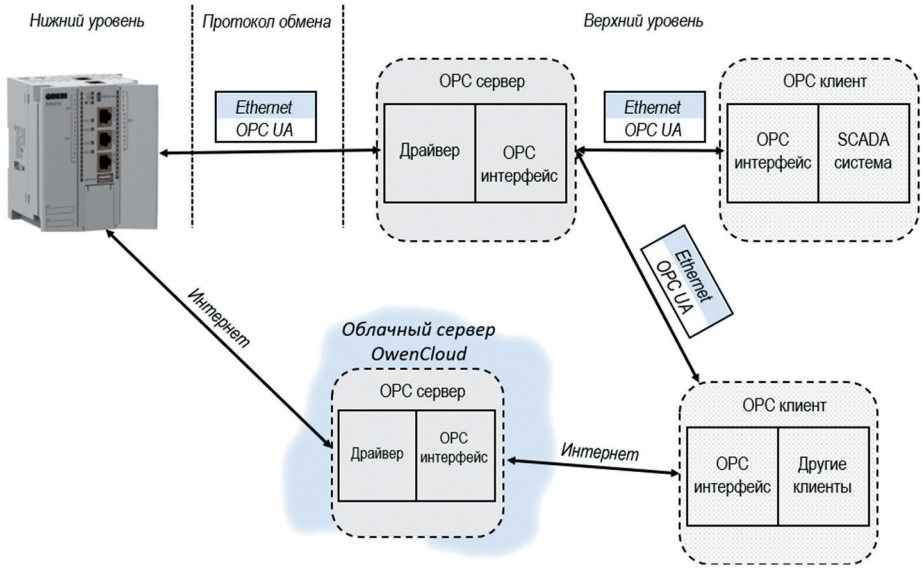

Рис.1. Структурная схема взаимодействия клиентов и серверов *OPC UA*

программного обеспечения спецификаций OPC *UA*, определяет независимость потребителей от наличия или отсутствия драйверов или протоколов. Широкая возможность выбора оборудования и программного обеспечения позволяет поддерживать соответствие характеристик систем и реальных потребностей заказчиков разработок. Схема взаимодействия клиентов и серверов OPC *UA* представлена на схеме (рис. 1).

На нижнем уровне промышленный контроллер собирает данные с датчиков и других источников информации. Контроллер подключен к серверу через протокол *Ethernet* и для передачи данных использует стандарты OPC *UA*. На верхнем уровне OPC сервер принимает данные от контроллера через драйвер и обеспечивает их обработку и хранение. Сервер предоставляет интерфейс OPC для взаимодействия с клиентами. Это могут быть системы *SCADA* или другие клиентские приложения и системы управления. Они используют данные, предоставленные сервером, для мониторинга и управления производственными процессами.

Стандарты OPC *UA* позволяют использовать облачные технологии (например, облачный сервер *OwenCloud*). Данный сервер взаимодействует с локальным OPC сервером и предоставляет возможность удаленного доступа клиентам через Интернет. Клиенты могут быть расположены в разных географических зонах и получать данные через интерфейс *OPC*.

Глубокая проверка пакетов данных (*Deep Packet Inspection* (*DPI*)) – это технология, которая позволяет анализировать как заголовки, так и содержимое пакетов данных, проходящих через точку инспекции. В отличии от традиционного метода инспекции пакетов, который фокусирует только заголовки пакетов, *DPI* обеспечивает анализ элементов передаваемых сообщений, позволяя идентифицировать, контролировать и фильтровать данные, а также проводить их детальную обработку, например, приоритизацию трафика, блокировку вредоносного контента, управление сетевыми ресурсами и обеспечение соблюдения политик безопасности [5].

Рис. 2. Алгоритм реализации принципов работы *DPI*

В структуре модели *Open System Interconnection* (*OSI*) технология *DPI* применима начиная с 2 по 7 уровень (уровень приложений), проводя анализ данных в пакетах, которые перемещаются по сетевой инфраструктуре [2]. Технологию *DPI* предлагается реализовывать с помощью аппаратных средств ОРС или в виде программного обеспечения, внедренного в такие устройства как маршрутизаторы, брандмауэры или независимые системы, в частности серверы ОРС. Принципы работы *DPI* предлагается рассматривать на примере алгоритма, представленного на рис. 2.

Предлагаемый алгоритм построения *DPI* включает ряд последовательных этапов.

На первом этапе инициализируется захват пакетов на сетевом уровне, после чего проводится анализ заголовков пакетов с целью определения адресов источника и приемника, а также других параметров. Далее следует этап анализа содержимого пакетов, на котором осуществляется сканирование конкретных данных для выявления вредоносных компонентов. На основании полученной информации принимаются решения о дальнейших действиях в отношении пакетов (блокировка, перенаправление или приоритизация). Завершающим этапом является применение политик безопасности, согласно результатам проведенного анализа.

В целом технология *DPI* позволяет визуализировать трафик, определять узкие места и оптимизировать сетевые ресурсы. Анализ содержимого и метаданных пакетов помогает администраторам контролировать трафик, выявлять аномалии и планировать пропускную способность каналов связи. *DPI* также используется Интернет-провайдерами для соблюдения нормативных требований и регулирования трафика. В результате обнаружение киберугроз повышает врзможность обеспечения безопасности критически важных приложений и качества их использования.

2. Особенности применения DPI в работе OPC UA и методика расчета рисков ИБ

Важность системы стандартов ОРС *UA* определяется регламентацией условий для обеспечения надежной и безопасной передачи данных в промышленных автоматизированных системах. На каждом из этапов жизненного цикла АСУ оценка живучести этой системы управления осуществляется посредством идентификации рисков и оценки параметров ее работы на соответствие нормативным критериям. Далее ставится задача минимизации рисков с помощью введения контрмер, устраняющих уязвимости, связанные с воздействиями внешних факторов. Для контроля динамики рисков в данной работе предлагается алгоритм, основанный на учете развития угроз, а также для оценки действенности контрмер по каждому элементу АСУ.

В соответствии методологическими нормами ИСО/МЭК 15408-1 предлагаются этапы расчета рисков при внешних воздействиях на систему автоматизации:

Первый этап – рассчитывается уровень угроз (R) по уязвимостям (U) на основе критичности и вероятности реализации угрозы внешних воздействий через данные уязвимости. Уровень угроз показывает, насколько критичным является воздействие каждой угрозы на объект защиты с учетом вероятности ее реализации.

Уязвимость при режиме работы с одной базовой угрозой: $U = \frac{E_R}{100} \times \frac{p(V)}{100}$, где *:* E_R – критичность реализации угрозы R (%); $P(U)$ – вероятность реализации R при уязвимости U (%).

Значения уровня R находятся в интервале от 0 до 1.

Второй этап – рассчитываются уровни угроз при всех уязвимостях U, через которые возможна реализация R на данном объекте, Итоговые уровни угроз через конкретные уязвимости вычисляются по формуле:

Уязвимость для режима с одной базовой угрозой (r):

$$U_r = 1 - \prod_{i=1}^{n} \left(1 - U_r^i\right),$$

где U_r^i – уровень r по уязвимостям $i = 1, 2..., n$. Значения уровней угроз при всех уязвимостях также получается в интервале от 0 до 1.

Аналогично рассчитывается общий уровень уязвимостей U, учитывающий все угрозы, действующие на объект, по формуле:

$$U = 1 - \prod_{r=1}^{R} \left(1 - U_r\right),$$

где U – уровень уязвимостей для всех угроз.

В рассмотрении функциональной надежности систем автоматизации важным параметром, значение которого зависит от эффективности применения технологии *DPI*, является ресурс системы (G). В данной работе примем, что для системы, имеющей ресурс G, риск Q рассчитывается как $Q = CU_G \times D$, где G – оценка ресурса системы ($G = 1 - P(G)$), где $P(G)$ – вероятность сбоев в передаче сообщений между ее элементами с адекватностью не ниже нормативной; D – критичность ресурса (безразмерный экспертный коэффициент задается количественно или качественно, исходя из цели применения объекта); U_G – общий уровень угроз по ресурсу G.

Если риск задается качественно, то для значения критичности берется оценка уровня. Например, для трех равномерных уровней:

Название уровня	Оценка уровня, %
1	33,33
2	66,66
3	100

Для угрозы доступность (отказ в обслуживании) критичность ресурса в год назначается, исходя из следующих оценок: $D_{а/год} = D_{а/час} \times T_{max}$, где $D_{а/год}$ – критичность ресурса в год*;* $D_{а/час}$ – критичность ресурса в час; T_{max} – максимальное критичное время проведения транзакций в год.

Риск по АСУ R_S рассчитывается по формулам:

Для количественного расчета риска: $R_S = \sum_i^n R_S^i$, где: R_S – риск по ресурсу. Для качественного расчета риска:

$$R_C = \left[1 - \prod_{i=1}^{n}\left(1 - \frac{R_c^i}{100}\right)\right] \times 100,$$

где R_c – риск по составу АСУ.

Однако с расширением цифровизации промышленных систем и повсеместным подключением их к Интернету возрастают и потенциальные угрозы безопасности [3, 6]. К наиболее существенным угрозам в области информационной безопасности можно отнести:

• кибератаки, целью которых является изменение нормального хода производственных процессов за счет внедрения вредоносного ПО системы управления и мониторинга;

• несанкционированный доступ к защищенной информации в сети предприятия, что может привести к утечке коммерческой тайны или другой важной информации;

• атаки на такие компоненты сети как DDoS-атаки, которые могут вывести из строя элементы инфраструктуры, вызывая остановку технологического процесса или другие сбои в работе систем управления [5];

• неустраненные ошибки в системах аутентификации и авторизации, которые могут быть использованы для несанкционированного доступа к системам управления и мониторинга.

Примерами кибератак в сетях OPC *UA* являются: кибератака *Stuxnet* [87], нацеленная на программируемые логические контроллеры, вредоносное программное обеспечение *Havex* [8], которое было использовано для сбора данных и саботажа в промышленных системах, кибератака *BlackEnergy* на крупные энергосистемы в том числе через протоколы OPC *UA* [9]. Такие инциденты подчеркивают необходимость укрепления защиты информации. Технологии *DPI* в промышленных автоматизированных системах на основе OPC *UA* помогают обнаруживать и предотвращать такие атаки, благодаря наличию функций детального анализа сетевого трафика в промышленных сетях [10].

3. Особенности размещения *DPI* в промышленной сети OPC *UA*

В качестве одного из комплексных решений организации применения технологии глубокой проверки пакетов информации в открытой распределенной системе данных на рис. 3 представлена структурная схема размещения *DPI* в промышленной сети взаимодействия клиентов и серверов OPC *UA*. Выделены 3 наиболее уязвимые точки:

1) *DPI* задействована для анализа всего трафика, передаваемого от контроллера к серверу OPC. Точка дает возможность выявления аномалий или злонамеренного трафика, исходящего из нижележащих слоев сети.

2) *DPI* применяется для мониторинга обмена данными между сервером и клиентами, включая системы *SCADA*. Точка позволяет противодействовать атакам на уровне передачи данных между сервером и клиентскими приложениями.

3) *DPI* предназначена для анализа коммуникаций между облачным сервером и другими элементами сети, что критически важно для предотвращения атак, направленных на облачные ресурсы, а также для защиты данных, транслируемых через Интернет в закрытый сегмент сети.

Предлагаемое расположение аппаратно-программных комплексов *DPI* обеспечивает возможность контроля и защиты критически важных точек передачи данных в системе, гарантируя комплексную безопасность сетевой архитектуры на основе OPC *UA*.

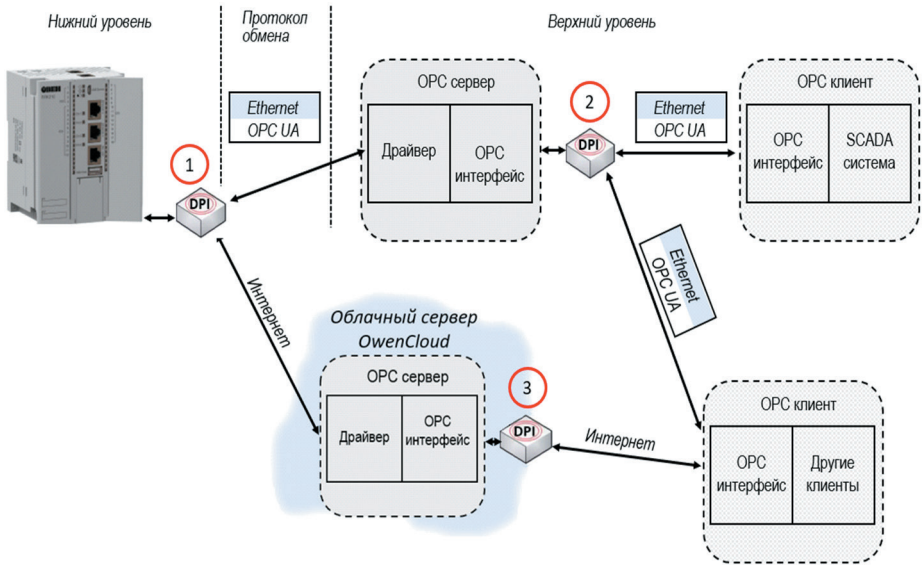

Рис. 3. Место DPI в схеме взаимодействия клиентов и серверов OPC UA

Заключение

Проведенный анализ показал, что существующие системы OPC *UA* подвержены таким угрозам, как кибератаки на уровне управления и мониторинга, утечки конфиденциальных данных и *DDoS*-атаки. Сложности и ограничения, которые возникают в процессе интеграции технологии *DPI* в архитектуру OPC *UA*, предлагается классифицировать по двум категориям.

Во-первых, технические и эксплуатационные аспекты. Внедрение *DPI* требует глубоких изменений в структуре и настройках сетевых устройств и программного обеспечения. Это сложные и трудоемкие задачи, выходящие за рамки компетенции персонала. Использование *DPI* повышает нагрузку на сетевые ресурсы за счет необходимости тщательной обработки каждого передаваемого пакета данных, что приводит к снижению производительности сети и увеличению времени задержки передаваемого сообщения. Интеграция *DPI* с существующими системами OPC *UA* может потребовать модернизации или замены некоторых компонентов системы, что также влечет за собой дополнительные расходы и временные затраты.

Во-вторых, при обеспечении совместимости и производительности технология *DPI* должна быть адаптирована к использованию с различными протоколами OPC *UA*. Для достижения эффективного уровня анализа и защиты данных может потребоваться индивидуальная настройка для каждого конкретного протокола. Повышенная нагрузка на устройства *DPI* может сказаться на их производительности и удлинить процесс анализа данных, потому важно найти баланс между глубиной анализа данных и производительностью системы. Кроме того, необходимость в регулярном обновлении базы сигнатур и правил фильтрации данных требует постоянного внимания и поддержки со стороны специалистов в области информационной безопасности.

Опыт применения разработанной схема интеграции программно-аппаратных комплексов *DPI* в промышленную сеть на основе стандартов OPC *UA* с учетом возникающих сложностей позволяет: выявлять скрытые угрозы при детальном анализе содержимого пакетов; блокировать вредоносный трафик при обнаружении атак по сигнатурам; идентифицировать аномалии, указывающие на вторжение злоумышленника, путем применения поведенческого анализа трафика; фильтровать и блокировать нежелательный трафик с высокой точностью.

Внедрение технологии *DPI* и инструментов, предоставляемых ею в инфраструктуру OPC *UA*, позволяет повысить уровень безопасности и надежности промышленных автоматизированных систем. *DPI* позволяет улучшить анализ сетевого трафика, за счет учета аномалии трафика в рамках конкретного протокола. Применение данной технологии в промышленных сетях позволяет выявлять основные факторы, требующие дополнительного изучения при внедрении *DPI*: сложность интеграции, большая нагрузка на сеть и необходимость обновления отдельных элементов системы, в ряде случаев необходимость реализации аппаратно-программных компонентов со стороны производителя систем промышленной автоматизации. Важно учитывать необходимость регулярного обновления баз данных сигнатур и правил фильтрации. Разработанная схема размещения *DPI* в сети OPC *UA* показывает, как этот программно-аппаратный комплекс применяется для обеспечения безопасности на всех уровнях взаимодействия.

В целом, можно сделать вывод, что интеграция *DPI* в OPC *U*A является действенной стратегией при повышении уровня безопасности и надежности промышленных автоматизированных систем в современных условиях интеграции сети Интернет в промышленных решениях при растущем числе киберугроз.

Библиографический список

1. Чаус Е.А. Концепция и базовый подход к построению системы защиты информации в многоуровневой интеллектуальной системе управления предприятием // Евразийское объединение. Оригинальная статья https://doi.org/10.21683/1729-2646-2024-24-3-52-60. 2020, 10-2 (68), с. 157-159.

2. Романенко О.А. Глубокая инспекция пакетов как средство анализа и контроля трафика. Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных. // В сб.: Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных : материалы Междун. науч.-технич. семинара, Минск, ноябрь-декабрь 2018 г. / Редкол.: М. Н. Бобов [и др.]. Минск: БГУИР, 2018. С. 90–93.

3. Панин Д.Н., Бобков Е.О., Балашова Е.А. Анализ кибератак на критическую информационную инфраструктуру с IOT технологиями // Автономия личности. 2020. № 2(22). С. 55-64.

4. Юркевич Е.В., Крюкова Л.Н. Проблемы нормативного обеспечения функциональной надежности цифрового производства // Надежность. 2024. Т. 24. № 3. С. 52-60. DOI: 10.21683/1729-2646-2024-24-3-52-60

5. Вейбер В.В., Кудинов А.В., Марков Н.Г. Задача сбора и передачи технологической информации распределенного промышленного предприятия // Известия ТПУ. 2011. № 5. С. 69-74.

6. Камышев С.В., Карманов И.Н. Проблемы DDoS-атак в современной IT-индустрии и методы защиты от них // Интерэкспо Гео-Сибирь. 2018. № 9. С. 121-125.

7. Langner R. Stuxnet: Dissecting a cyberwarfare weapon // IEEE Security & Privacy. 2011. Vol. 6. Iss. 3. Pp. 49–51. DOI: 10.1109/MSP.2011.67

8. Takagi H., Morita T., Matta M. et al. Strategic security protection for industrial control systems // In: Society of Instrument and Control Engineers of Japan (SICE), 2015 54th Annual Conference. IEEE, 2015. Pp. 986-992.

9. Khan R., Maynard P., Mclaughlin K. et al. Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid // In: 4th

International Symposium for ICS & SCADA Cyber Security Research 2016. DOI: 10.14236/ewic/ICS2016.7

10. Кузьмин В.Н., Менисов А.Б. Исследование путей и способов повышения результативности выявления компьютерных атак на объекты критической информационной инфраструктуры // Информационно-управляющие системы. 2022. № 4. С. 29–43. DOI: 10.31799/1684-8853-2022-4-29-43

References

1. Chaus E.A. [Concept and basic approach to building an information protection system in a multilevel intelligent enterprise management system]. *Eurasian Scientific Association* 2020;10-2(68):157-159. (in Russ.)

2. Romanenko O.A. [Deep packet inspection as a means of traffic analysis and control]. In: Telecommunications: networks and technologies, algebraic coding, and data security]. (accessed 30.06.2024). Available at: https HYPERLINK "https://libeldoc.bsuir.by/bitstream/123456789/36300/1/Romanenko_Glubokaya.pdf.

3. Panin D.N., Bobkov E.O., Balashova E.A. Analysis of cyber-attacks on critical information infrastructure with IoT technologies. *The Autonomy of Personality* 2020;2(22):55-64. (in Russ.)

4. Yurkevich E.V., Kryukova L.N. Matters of assuring functional dependability compliance of digital manufacturing. *Dependability* 2024;24(3):52-60. (in Russ.) DOI: 10.21683/1729-2646-2024-24-3-52-60.

5. Weiber V.V., Kudinov A.V., Markov N.G. [The task of collecting and transmitting technological information of a distributed industrial enterprise]. *TPU News* 2011;5. (accessed 29.06.2024). Available at: https://cyberleninka.ru/article/n/zadacha-sbora-i-peredachi-tehnologicheskoy-informatsii-raspredelennogo-promyshlennogo-predpriyatiya. (in Russ.)

6. Kamyshev S.V., Karmanov I.N. Problem of DDoS attacks in modern IT-industry and methods of protection against them. *Interexpo GEO-Siberia* 2018;9:121-125. (in Russ.)

7. Langner R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy* 2011;6(3):49-51. DOI: 10.1109/MSP.2011.67.

8. Takagi H., Morita T., Matta M. et al. Strategic security protection for industrial control systems. In: Society of Instrument and Control Engineers of Japan (SICE), 2015 54th Annual Conference. IEEE; 2015. Pp. 986-992.

9. Khan R., Maynard P., McLaughlin K. et al. Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. In: 4th International Symposium for ICS & SCADA Cyber Security Research; 2016. DOI: 10.14236/ewic/ICS2016.7.

10. Kuzmin V.N., Menisov A.B. A study of ways and solutions to increase the efficiency of detecting computer attacks on the objects of critical information infrastructure. I*nformatsionno-upravliaiushchie sistemy* 2022;4:29-43. (in Russ.). DOI:10.31799/1684-8853-2022-4-29-43.

Сведения об авторах

Чаус Евгений Александрович – ведущий инженер по автоматизированным системам управления производством, специалист в области стандартизации средств и систем автоматизации технологических процессов. ПАО «Группа Черкизово», Российская Федерация, Москва, e-mail: zc86@mail.ru

Юркевич Евгений Владимирович – д.т.н., профессор, главный научный сотрудник ИПУ РАН специалист в области функциональной надежности и системного анализа. Институт проблем управления имени В.А.Трапезникова Российской академии наук, Российская Федерация, Москва, e-mail: 79163188677@yandex.ru

About the authors

Evgeny A. Chaus, Lead Engineer, Automated Production Control Systems, expert in standardisation of process automation equipment and systems. Cherkizovo Group, Russian Federation, Moscow, e-mail: zc86@mail.ru

Evgeny V. Yurkevich, Doctor of Engineering, Professor, Head Researcher, ICS RAS, expert in functional dependability and systems analysis. V.A. Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Russian Federation, Moscow, e-mail: 79163188677@yandex.ru

Вклад авторов в статью

Чаус Е.А. разработал алгоритм реализации принципов работы DPI в сегменте промышленного протокола OPC UA. Показал особенности размещения узлов DPI в промышленной сети OPC UA.

Юркевич Е.В. предложил методику расчета рисков при внешних воздействиях на систему автоматизации в рамках использования механизмов DPI в промышленной сети OPC UA.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.