В последнее время особое внимание уделяется вопросам информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП), стоящих на страже критически важных производственных операций. Статьи, опубликованные на порталах CNews [6] и Anti-Malware [7], подчёркивают сложности, с которыми сталкиваются специалисты при защите этих систем от киберугроз и аварий. С одной стороны, акцентируется нехватка практически эффективных решений для надёжной защиты, несмотря на ужесточение законодательных требований и рост числа информационных атак. С другой стороны, поднимается вопрос актуальности и эффективности существующих средств обнаружения вторжений (СОВ) в контексте ускоренной цифровизации и модернизации промышленных предприятий.

Исследования сосредотачиваются на функциональности средств обнаружения, требованиях к ним и их способности обнаруживать угрозы и аномалии. Важным аспектом является анализ трафика и контроль за состоянием оборудования. Обсуждаются также вопросы удобства использования и возможности интеграции с другими системами безопасности.

Среди отечественных решений выделяется система DATAPK, разработанная компанией УЦСБ и сертифицированная ФСТЭК России. Этот инструмент обеспечивает комплексный подход к защите АСУ ТП, включая непрерывный мониторинг защищаемых объектов, автоматизированную инвентаризацию, управление событиями безопасности и выявление сетевых аномалий, что подробно рассказывается в вебинаре «DATAPK: на страже АСУ ТП» [4]. Особенностью DATAPK является способность интегрировать анализ разнородных данных для создания полной картины информационной безопасности, что демонстрирует практическую значимость системы на примерах её внедрения. Более подробно это описано на официальном сайте UDV Group [2].

Анализ различных СОВ, проведённый компанией «Инфосистемы Джет», показал, что важными критериями выбора являются их функциональность, способность обеспечивать защиту от угроз, соответствие нормативным требованиям и возможность интеграции с другими средствами защиты. В исследовании участвовали решения от ведущих производителей, включая DATAPK, что подчёркивает значимость разработки в контексте обеспечения кибербезопасности АСУ ТП [10].

Статьи акцентируют важность централизованного и комплексного подхода к обеспечению информационной безопасности в современных условиях, подчёркивая роль отечественных разработок, сертифицированных российскими регуляторами, в укреплении защиты промышленных объектов от киберугроз. Особое внимание уделяется тренду на импортозамещение и поддержке отечественных инноваций, способствующих повышению уровня информационной безопасности в ключевых отраслях экономики.

По информации с официального сайта UDV Group [7], Компания СайберЛимфа, являющаяся частью UDV Group [1], официально объявила о получении сертификата соответствия ФСТЭК России для своего программного комплекса CyberLympha DATAPK, также известного на рынке под торговым наименованием UDV DATAPK Industrial Kit [3]. Получение сертификата №4719 от 28 сентября 2023 года является значимым событием для компании и для рынка информационной безопасности в целом, подтверждая высокий уровень доверия к решению и его соответствие строгим требованиям Федеральной службы по техническому и экспортному контролю России.

Программный комплекс CyberLympha DATAPK разработан для обеспечения защиты важных объектов критической информационной инфраструктуры и систем управления производственными и технологическими процессами [9]. Это включает в себя объекты, которые могут представлять угрозу для жизни и здоровья людей или для окружающей среды. Сертификат подтверждает соответствие продукта требованиям по шестому уровню доверия, требованиям к средствам обнаружения вторжений, профилям защиты средств обнаружения вторжений для сетей шестого класса защиты и заданию по безопасности.

Основные задачи, на решение которых направлен UDV DATAPK Industrial Kit, включают мониторинг состояния защищенности промышленных сетей, выявление инцидентов информационной безопасности в системах промышленной автоматизации и выполнение требований законодательства РФ в области информационной безопасности. Это охватывает требования к уровням доверия, профилю защиты, а также реализацию мер по идентификации и аутентификации пользователей и устройств, управлению учётными записями в соответствии с заданием по безопасности.

Получение сертификата соответствия от ФСТЭК России ставит продукт в ряд ведущих решений в сфере обеспечения безопасности критической информационной инфраструктуры и АСУ ТП, подчеркивая его способность соответствовать высоким стандартам защиты и эффективности в борьбе с угрозами кибербезопасности. Это также отражает растущую значимость комплексных подходов к защите информационных систем в условиях постоянно развивающегося ландшафта угроз и повышает доверие к отечественным разработкам в области информационной безопасности.

Статья, опубликованная на сайте Anti-Malware.ru под авторством Сергея Лыдина [8], представляет собой обзор программно-аппаратного комплекса DATAPK, разработанного компанией «Уральский центр систем безопасности» (ООО «УЦСБ»). DATAPK предназначен для мониторинга и контроля за состоянием защищённости автоматизированных систем управления технологическими процессами (АСУ ТП), применяемых на объектах критической информационной инфраструктуры и других значимых производствах. Особое внимание в статье уделено выявлению несанкционированных изменений, регистрации событий, выявлению уязвимостей в компонентах и обнаружению попыток их эксплуатации, а также автоматизированному контролю выполнения требований по информационной безопасности.

Продолжая тему информационной безопасности и важности анализа сетевого трафика, в последующих материалах освещается ряд ключевых моментов и разработок в данной области. Статьи делают акцент на продвижении и улучшении систем анализа сетевого трафика (NTA), выделяя их роль в обнаружении и предотвращении киберугроз.

В обзоре мирового и российского рынка NTA подчёркивается, что спрос на такие системы постоянно растёт в связи с увеличением числа и сложности кибератак. Авторы отмечают, что на российском рынке существует потребность в развитии отечественных NTA-систем, способных конкурировать на мировом уровне, при этом подчёркивается значимость таких систем для обеспечения национальной безопасности. Отмечается, что эффективность NTA-систем зависит от их способности анализировать широкий спектр сетевого трафика и выявлять как известные, так и новые угрозы. Развитие алгоритмов машинного обучения и искусственного интеллекта играет ключевую роль в улучшении функционала NTA и повышении уровня обнаружения аномалий и атак.

Сергей Лыдин подробно рассматривает архитектуру DATAPK, его функциональные возможности, объекты защиты и сертификацию. Комплекс может функционировать в разных режимах, включая пассивный и активный мониторинг, а также сканирование защищённости. DATAPK обладает широкими возможностями для управления идентификаторами, сбора и хранения информации о событиях безопасности, мониторинга, выявления уязвимостей и обеспечения контроля за составом аппаратуры и программного обеспечения. Он также поддерживает автоматическое обнаружение и идентификацию инцидентов, управление изменениями конфигурации АСУ ТП и документирование информации о данных изменениях.

Помимо технических аспектов, рассматривается также вопрос организационной структуры и методов работы аналитических команд в сфере информационной безопасности. Управление событиями безопасности (SIEM) и NTA совместно играют важную роль в процессе обнаружения и реагирования на киберугрозы, необходимо обеспечить их эффективное взаимодействие и интеграцию для достижения наивысшего уровня защиты информационных ресурсов .

Преимуществами DATAPK, выделенными в статье, являются комплексный анализ данных из различных источников, определение текущего состава компонентов АСУ ТП, обнаружение компьютерных атак, идентификация и контроль доступа к системе. Комплекс предлагает гибкие решения для адаптации под конкретные нужды пользователя без изменения программного кода, обладая различными вариантами исполнения аппаратной платформы для создания распределённой иерархии.

Недостатками, отмеченными автором, являются громоздкий пользовательский интерфейс, отсутствие простого варианта полного развёртывания с помощью мастера и недоступность тонкой настройки через веб-интерфейс без использования внешних конфигурационных файлов.

В статье делается вывод о необходимости реализации комплекса мер по мониторингу безопасности в АСУ ТП, подчёркивая значимость таких систем для обеспечения безопасного и непрерывного функционирования информационно-телекоммуникационных систем и сетей. DATAPK представлен как продукт, способный решить множество актуальных задач информационной безопасности, обладающий рядом успешных внедрений, включая проекты для ПАО «Северсталь».

Системы анализа сетевого трафика (NTA) являются ключевым инструментом для выявления угроз ИБ на ранней стадии атаки, что подробно описываетя в статье Александра Панасенко [11]. Они обеспечивают возможность оперативно локализовать угрозы и контролировать соблюдение норм ИБ, представляя значительное преимущество перед традиционными примитивными средствами защиты. Также отмечается необходимость в развитии NTA-систем, способных анализировать сетевой трафик на глубоком уровне, выявлять нестандартные паттерны поведения и обеспечивать защиту не только на периметре, но и внутри сетевой инфраструктуры организации. Это включает использование машинного обучения, поведенческий анализ, а также ретроспективный анализ данных для выявления и предотвращения угроз. Представлены кейсы использования NTA-систем, подчеркивающие их эффективность в обнаружении атак, ошибок в конфигурации сети и нарушений корпоративных политик. Среди примеров использования NTA-систем — расшифровка цепочки атак, локализация угрозы и принятие компенсационных мер, а также помощь в активном поиске угроз (threat hunting).

Так же обсуждаются перспективы развития NTA, в том числе необходимость новых подходов к анализу трафика, улучшенных методов выявления угроз и возможности хранения и экспорта данных для детального анализа и расследования инцидентов. Подчеркивается, что NTA является важной частью современных центров обработки данных (SOC), наряду с SIEM и EDR, и требует дальнейшего развития для удовлетворения растущих потребностей в области кибербезопасности

Несмотря на преимущества, существующие NTA-системы сталкиваются с рядом ограничений, включая недостаточное покрытие функциональности и необходимость более глубокого анализа сетевого трафика для эффективного обнаружения и расследования компьютерных инцидентов. Более подробно это описывается в статье на сайте Ptsecurity [12]. Наблюдается потребность в разработке и внедрении новых подходов к анализу трафика, улучшении методов детектирования угроз и обеспечении возможности хранения и экспорта данных для последующего анализа.

По информации из статьи на сайте habr [14], cистемы анализа сетевого трафика (NTA) играют критическую роль в обнаружении угроз информационной безопасности, анализируя события на уровне сети. Они позволяют выявлять действия злоумышленников на ранней стадии атаки, оперативно локализовать угрозы и контролировать соблюдение нормативов информационной безопасности.

Совокупность представленных материалов подчеркивает значимость развития и внедрения современных технологий в области информационной безопасности. Инструменты, такие как Zeek и DATAPK, вместе с продвинутыми NTA-системами, играют ключевую роль в обнаружении и предотвращении киберугроз, обеспечивая защиту критически

В статье на сайте securitylab [13] рассказывается, что системы анализа сетевого трафика (NTA) играют ключевую роль в обеспечении безопасности информационных систем и сетей. Различие между NTA, IDS, UTM и NGFW заключается в специфике их применения и функциональных возможностях. В то время как IDS (системы обнаружения вторжений) сосредоточены на выявлении угроз на основе известных подписей атак, NTA используют сложные алгоритмы для анализа сетевого трафика в реальном времени, чтобы идентифицировать аномалии, указывающие на возможные угрозы. В статье о системах анализа сетевого трафика подчёркивается, что NTA-системы должны обладать способностью не только обнаруживать известные угрозы, но и идентифицировать неизвестные или адаптированные атаки. Это требует от систем NTA использования сложных алгоритмов машинного обучения и искусственного интеллекта для анализа сетевого трафика и выявления аномалий, которые могут указывать на наличие угроз.

Одним из примеров эффективного использования NTA-систем является Zeek (ранее известный как Bro), который предоставляет детальный анализ сетевого трафика, позволяя обнаруживать и предотвращать киберугрозы на ранних стадиях. Zeek отличается высокой гибкостью и настраиваемостью, что делает его мощным инструментом в руках специалистов по кибербезопасности. Более подробно можно изучить информацию на официальном сайте Zeek [15].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. UDV Group : официальный сайт. – Екатеринбург – . – URL: https://udv.group/ (дата обращения: 20.02.2024). – Текст : электронный.
2. UDV DATAPK Industrial Kit : официальный сайт. – Екатеринбург – Обновляется в течение суток. – URL: https://udv.group/products/udv-datapk-industrial-kit/ (дата обращения: 20.02.2024). – Текст : электронный.
3. Руководство пользователя Cyberlympha : сайт. – Екатеринбург – . – URL: [https://docs.cyberlympha.com/datapk/ru/19/](https://docs.cyberlympha.com/datapk/ru/19/%20) (дата обращения: 20.02.2024). – Текст : электронный.
4. Вебинар «DATAPK: на страже АСУ ТП» – УЦСБ – УЦСБ : сайт. – Екатеринбург – . – URL: [https://www.ussc.ru/events/zapisi-vebinarov/vebinar-datapk-na-strazhe-asutp/](https://www.ussc.ru/events/zapisi-vebinarov/vebinar-datapk-na-strazhe-asutp/%20) (дата обращения: 20.02.2024). – Текст. Изображение : электронные.
5. CNews : сайт / Какие решения защищают промышленность от киберпреступников и катастроф – Екатеринбург – . – URL: [https://safe.cnews.ru/articles/2020-09-07\_kakie\_resheniya\_zashchishchayut\_promyshlennost](https://safe.cnews.ru/articles/2020-09-07_kakie_resheniya_zashchishchayut_promyshlennost%20) (дата обращения: 20.03.2024). – Текст : электронный.
6. Anti-malware : сайт / Сравнение промышленных средств обнаружения вторжений (СОВ/IDS для АСУ ТП) – Москва – . – URL: [https://www.anti-malware.ru/compare/Intrusion-Detection-Systems](https://www.anti-malware.ru/compare/Intrusion-Detection-Systems%20) (дата обращения: 12.03.2024). – Текст. Изображение : электронные.
7. UDV Group : официальный сайт / UDV DATAPK Industrial Kit получил сертификат соответствия ФСТЭК России – Екатеринбург – . – URL: https://udv.group/about/news/udv-datapk-industrial-kit-poluchil-sertifikat-sootvetstviya-fstek-rossii/ (дата обращения: 12.03.2024). – Текст : электронный.
8. Anti-malware : сайт / Лыдин С. – Обзор DATAPK – комплекса оперативного мониторинга и контроля защищённости АСУ ТП – Москва – . – URL: https://www.anti-malware.ru/reviews/PAK-DATAPK (дата обращения: 12.03.2024). – Текст. Изображение : электронные.
9. Habr : сайт / Киберфизические системы в безопасности. Как устроен стартап CyberLympha, выходящий на сингапурский рынок – Москва – . – URL: [https://habr.com/ru/companies/generations/articles/715096/](https://habr.com/ru/companies/generations/articles/715096/%20) (дата обращения: 20.03.2024). – Текст. Изображение : электронные.
10. Tadviser : сайт / DATAPK (tadviser.ru) – Москва – . – URL: [https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:DATAPK?ysclid=lkj9p46qtx985802210](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:DATAPK?ysclid=lkj9p46qtx985802210%20) (дата обращения: 20.03.2024). – Текст. Изображение : электронные.
11. Anti-malware : сайт / Панасенко А. – Системы анализа сетевого трафика (NTA) – обзор мирового и российского рынка – Москва – . – URL: <https://www.anti-malware.ru/analytics/Market_Analysis/Global-and-Russian-market-Network-Traffic-Analysis-systems-review> (дата обращения: 25.03.2024). – Текст. Изображение : электронные.
12. Ptsecurity : сайт / Что такое network traffic analysis и зачем нужны NTA-системы – Москва – . – URL: <https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-network-traffic-analysis-i-zachem-nuzhny-nta-sistemy/> (дата обращения: 25.03.2024). – Текст. Изображение : электронные.
13. Securitylab : сайт / NTA, IDS, UTM, NGFW — в чем разница– Москва – . – URL: https://www.securitylab.ru/analytics/517592.php (дата обращения: 25.03.2024). – Текст. Изображение : электронные.
14. Habr : сайт / NTA здорового человека: что должны уметь системы анализа сетевого трафика (и пока что не умеют) – Москва – . – URL: <https://habr.com/ru/companies/solarsecurity/articles/523460/> (дата обращения: 25.03.2024). – Текст. Изображение : электронные.
15. Zeek : официальный сайт / An Open Source Network Security Monitoring Too (zeek.org) – Сент-Джордж – . – URL: https://zeek.org/ (дата обращения: 25.03.2024). – Текст : электронный.