Письмо: PIR PRESS NEWS - Security Index Journal: Matvey Voytov on cybersecurity of critical infrastructure

22.07.2016
PIR PRESS NEWS - Security Index Journal: Matvey Voytov on cybersecurity of critical infrastructure

МОСКВА, 22 ИЮЛЯ. ПИР-ПРЕСС – «Важной особенностью обеспечения промышленной кибербезопасности является то, что каждый проект такого рода уникален — так же, как и каждая промышленная инфраструктура, в которую просто невозможно установить некие стандартизированные продукты», – Матвей Войтов, Руководитель отдела продуктового маркетинга в департаменте защиты критических инфраструктур "Лаборатории Касперского".

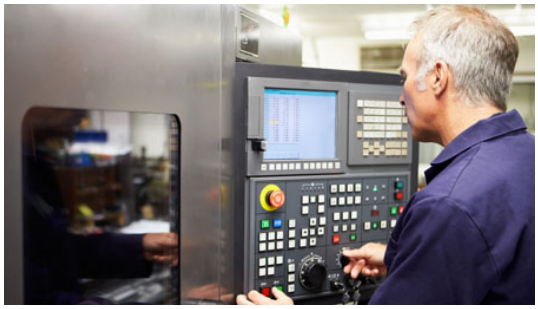
Внедрение информационно-коммуникационных технологий в повседневную жизнь государства и общества приносит значительную выгоду, положительно влияя на производительность труда и способствуя экономическому росту в целом. Однако многообразие возможных действий в киберпространстве и его доступность создают большой простор для деятельности лиц с далеко не благими намерениями.

Специалисты в области защиты критических инфраструктур отмечают, что за последние годы резко возросло количество кибернападений на промышленные предприятия и другие объекты критической инфраструктуры, а также повысилась сложность их исполнения. Успешная реализация подобной атаки, в зависимости от цели злоумышленников, может нанести государству значительный материальный ущерб или даже повлечь за собой негативные последствия для населения и окружающей среды.

Злоумышленники могут оказать воздействие на автоматизированную систему управления оборудованием даже если объект критической инфраструктуры не подключен к интернету. Такие противоправные действия могут стать элементом полномасштабной кибервойны, в которой могут участвовать как государства, так и негосударственные субъекты.

Руководитель отдела продуктового маркетинга в департаменте защиты критических инфраструктур *Лаборатории Касперского* Матвей **Войтов** в своем комментарии "Критическая инфраструктура в контексте кибербезопасности" разъясняет, какие именно объекты инфраструктуры включают в перечни критической инфраструктуры и кто их составляет, на каких принципах основано управление технологическим процессом на критически важных объектах, каким видам уязвимости они подвержены, и какие трудности представляет разработка и установка на них

систем защиты от киберугроз. Эксперт отмечает, что «подбор оптимальной конфигурации защитных технологий и набора сервисов осуществляется после полного обследования текущей системы безопасности промышленного объекта, а имплементация выбранных мер происходит только в специально отведенное технологическое окно, чтобы не повлиять на процесс работы системы».



По его словам, «важной особенностью обеспечения промышленной кибербезопасности является то, что каждый проект такого рода уникален — так же, как и каждая промышленная инфраструктура, в которую просто невозможно установить некие стандартизированные продукты». В статье отмечается, что чаще всего кибернападениям подвергаются объекты топливно-энергетического комплекса.

Статья опубликована в журнале «Индекс Безопасности» № 1 (116) 2016. Полный текст статьи доступен на сайте ПИР-Центра.

По вопросам, касающимся журнала «Индекс Безопасности», вы можете обращаться к главному редактору Ольге Мостинской по телефону +7 (495) 987 19 15 или по электронной почте mostinskaya@pircenter.org.

Тел.: +7 (495) 987-19-15
Адрес для писем: Россия, 119019, Москва, а/я 147

loading
Ошибка?
Обратите внимание на ош