

Все блоги / Новости Кода / Кибербезопасность промышленных систем. Новые вызовы

Кибербезопасность промышленных систем. Новые вызовы

Код ИБ INDUSTRIAL 2019

🕒 12 июля, 2019 по 📅 Кот ИБ | Комментариев пока нет



11 июля в рамках международной выставки ИННОПРОМ в Екатеринбурге впервые состоялась конференция по промышленной кибербезопасности Код ИБ INDUSTRIAL. Эксперты в сфере ИБ и инженеры АСУТП искали решения насущных вопросов, связанных с обеспечением безопасности промышленных систем и кадрами в отрасли.



Кот ИБ 12 июля 2019 г.

Модератором пленарной дискуссии, открывшей мероприятие, выступил Алексей Комаров (YLCB), который озвучил тезис о редкости возникновения инцидентов на промышленных предприятиях. Однако, эксперты дискуссии смогли привести факты, опровергающие это утверждение. Валерий Мельников (ФСТЭК) сообщил, что за прошлый год 48% компьютеров на предприятиях были подвержены атакам. По его данным, 38% атак из этого числа произошло через интернет, причиной 15-20% атак стало использование съемных носителей, и 2% - это фишинг. Антон Шипулин (RUSCADASEC) резонно отметил, что атак на крупный бизнес не проходит одновременно, она длится в течение продолжительного времени и начинается со сбора данных хакерами о компании. В это время ее крайне тяжело обнаружить, поэтому затишье в инцидентах на предприятии далеко не всегда означает отсутствие этих инцидентов. «Возможно как раз в этот самый момент на вас ведется атака», - заключил эксперт.

В этом вопросе согласие с ним высказал Павел Луцки (КриптоПро) рассказавший о своем опыте работы в крупном интеграторе, где спикер имел доступ к информации о реальных инцидентах. По его словам, инцидентов на промышленных предприятиях много, однако они редко становятся достоянием общественности, чаще всего это «тайна за семью печатями».

Обстоятельством, осложняющим ситуацию с выявлением атак, является малое количество разработанных средств, прошедших промышленную апробацию и способных обнаруживать атаки на ранних стадиях, считает Николай Навилов (Газинформсервис).

Руководитель Kaspersky Industrial CyberSecurity Алексей Петухов так комментирует защищенность промышленных предприятий: «Повсеместная цифровизация предприятия влечёт за собой киберриски. Информационная безопасность уже не является отдельно существующей службой. Она входит в общую систему управления рисками на предприятии, помогая автоматизировать и оптимизировать промышленные процессы и делать управление производством более эффективным. Например, недавно были опубликованы результаты отчёта аналитического агентства Forrester Consulting по применению на одном из предприятий решения Kaspersky Industrial CyberSecurity. Отчёт показал, что внедрение специализированного продукта для промышленных систем позволило снизить стоимость вынужденных простоев, связанных с ИТ системами. Сэкономленные расходы составили 1,7 миллиона долларов США».

Одним из современных вызовов промышленной кибербезопасности является безопасность интернета вещей. Эта сфера еще плохо регулируется законодательством, однако в свете повсеместной диджитализации приобрела огромный интерес со стороны производителей. «Успевает ли ИБ вслед за развитием IoT?», - задает вопрос модератор. Павел Луцки, опираясь на свой опыт, считает, что добиться хорошего результата в защищенности сферы интернета вещей возможно. Для этого должны быть объединены усилия и скоординированы действия ФСТЭК, ФСБ и представителей промышленности. «В рамках рабочей группы будет проще выработать общий всесторонний подход к обеспечению защиты сферы IoT», - высказал свое мнение эксперт.

Валерий Мельников сообщил, что подобный опыт в УрФО уже есть. В частности, создан Координационно-методический совет организаций лицензиатов ФСТЭК России. В рамках этой организации обсуждаются проблемы, с которыми сталкиваются компании-лицензиаты.

Кадровый вопрос послужил третьей темой для обсуждения экспертами конференции Код ИБ. Удручающую статистику привел Алексей Комаров. По данным ФСТЭК, в сфере информационной безопасности в России занято 22000 человек. Однако больше 75% этих сотрудников не имеют профессиональной квалификации в сфере ИБ. Лишь 5-10% прошли переподготовку, остальные имеют базовое образование в сфере ИБ.

Каждое предприятие, испытывающее нехватку кадров, по-своему решает этот вопрос. Но существует два универсальных способа: «хантинг», если кадры нужны срочно и возвращение специалистов из ВУЗов. Владимир Карантаев поделился опытом набора молодых специалистов в компании «Ростелеком»: «Взаимодействие с ВУЗами вполне дает результаты в решении кадровых вопросов. Мы охотно берем на работу успешных выпускников».

Завершилась дискуссия сессией вопросов и ответов к представителю регулятора, которым выступил Валерий Мельников, заместитель руководителя Управления ФСТЭК по УрФО. Он рассказал об ответственности субъектов КИИ, нарушающих сроки проведения процедур категорирования по 187-ФЗ, а также разъяснил основные положения приказов ФСТЭК в части регулирования законодательства о КИИ.

Впечатления участников

«Хорошая организация мероприятия, интересные темы докладов».
Дубровин Е.В / Таврия

«Разумная логика построения конференции. Интересный материал».
Погудин Р.А / УралЭнергоТел

«Интересно, полезно, новости в документах ФСТЭК очень кстати»
Шитова Наталья / Вуз-Банк

ПОДЕЛИТЬСЯ ЭТОЙ ЗАПИСЬЮ



НАШИ БЛОГИ

Новости компаний

Новости Кода

Код ИБ Академия

Итоги Кода

Публикации и статьи