Москва, 29 сентября - 1 октября

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ И ВЫСТАВКА

РЕЛЕЙНАЯ ЗАЩИТА И АВТОМАТИКА ЭНЕРГОСИСТЕМ 2021

Актуальные направления развития нормативной базы в области обеспечения кибербезопасности систем промышленной автоматизации

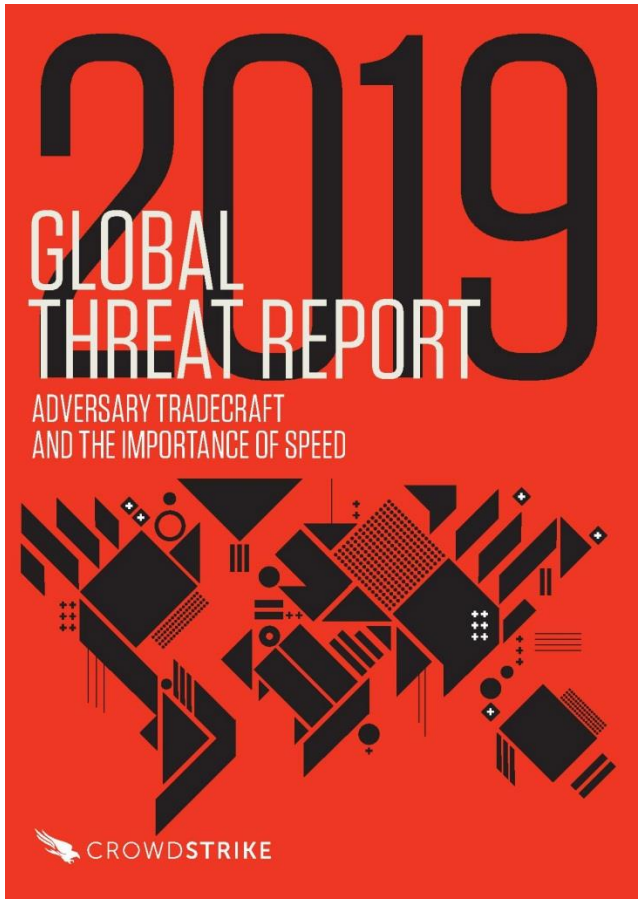
Д.И. Правиков

РГУ нефти и газа (НИУ) им. И.М.Губкина

Российская Федерация

«Время прорыва» (“breakout time”)

«Если вы не можете обеспечить скорость 1–10–60 (1 минута на обнаружение вторжения, 10 минут на расследование и 1 час на отражение и исправление ситуации), — считайте, что вы уже проиграли в этой войне».



Практика расследования

> … как показал опыт расследования киберинцидентов на промышленных предприятиях в первый момент времени очень трудно отличить изменение поведения управляемого оборудования, произошедшего в результате кибератаки, от сбоя, вызванного износом, отказом оборудования или неквалифицированным действием персонала.

Ян А. Сухих, Дмитрий И. Правиков, Алексей А. Кузичкин
РАЗРАБОТКА ЗАЩИЩЕННЫХ АРХИТЕКТУР АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ
// БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ = IT Security, Том 27, № 2 (2020)

Действующие требования

При получении информации о возникновении аварий, указанных в подпунктах "ж" - "н" пункта 4 настоящих Правил, субъект оперативно-диспетчерского управления в электроэнергетике уведомляет об этом уполномоченный орган в сфере контроля и надзора в электроэнергетике. Решение о расследовании причин аварии принимается не позднее 24 часов с момента получения уполномоченным органом в сфере контроля и надзора в электроэнергетике информации об аварии.

Правила расследования причин аварий в электроэнергетике (утверждены постановлением Правительства РФ от 28 октября 2009 г. № 846)

Опыт проведения занятий

Статистика по уязвимостям
Во время тренировки «Защита АСУТП предприятия – группа Х»
было закрыто уязвимостей - 1 из 3.
Далее приведено рекомендательное время устранения и фактическое время закрытия каждой из уязвимостей.
AXIS2
Рекомендуемое время: 90 мин
Фактическое время: 103 мин
COOLREADERPDF
Рекомендуемое время: 90 мин
Фактическое время: не устранена
IGSS32
Рекомендуемое время: 90 мин
Фактическое время: не устранена

выводы

Представляется целесообразным разработать проект требований к системам киберзащиты критической информационной инфраструктуры, обеспечивающей защиту от кибератак в начальный период воздействия, их парирование и восстановление. С учетом того, что построение таких систем возможно только с применением искусственного интеллекта, рассмотреть возможность внесения дополнений в Национальную стратегию развития искусственного интеллекта на период до 2030 года, утвержденную Указом Президента Российской Федерации от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации”

СПАСИБО ЗА ВНИМАНИЕ!

Контакты: dip@gubkin.pro