Промышленность под атакой
Насколько хорошо мы знаем своего врага?

Каракулин Сергей

10 факторов, влияющих на кибербезопасность предприятий

KASPERSKY

1

Эволюция технологических процессов

Необходимость производить новую, более сложную, продукцию изменяет требования к системам автоматизированного управления

2

Изменение процессов управления производством

Подъём функций мониторинга и управления на более высокие уровни иерархии

3

Постоянно возрастающая техническая сложность АСУ ТП

Переход на новые технологии при разработке систем автоматизированного управления

4

Уменьшение времени жизни АСУ ТП

Уменьшение длительности цикла разработки и поддержки продуктов для АСУ ТП

5

Повышение степени автоматизации, избавление от ручного труда

Рост общего количества систем автоматизации и прочих информационных систем на производстве

Увеличение разнообразия информационных систем, разработка и внедрение новых

Увеличение связности между системами

6

Укрупнение производств, покупки и слияния

7

Увеличение уровня защищённости «традиционных» жертв киберпреступников

Рост количества и качества используемых средств зашиты

Увеличение осведомлённости и зрелости процессов ИБ

Повышение доступности экспертизы в обнаружении и предотвращении атак

Рост уровня экспертизы органов охраны правопорядка в области
расследования киберпреступлений

8

Отсутствие очевидной повседневной угрозы

Оценить вероятность кибератаки и соответствующие риски не представляется возможным из-за недостатка статистики

Целевые атаки на АСУ ТП остаются экзотикой

Угроза атак нацеленных на кражу денег остаётся недооценённой

9

Неохотное раскрытие информации об уязвимостях, атаках и инцидентах

10

Геополитика

Проблемы кибербезопасности промышленных предприятий

KASPERSKY

1 Постоянно растущее количество и разнообразие уязвимостей и угроз

- Увеличение количества систем автоматизации
- Появление новых каналов связи для мониторинга и управления
- Увеличение количества организаций и лиц, имеющих доступ к системам автоматизации

2 Интерес со стороны киберкриминала и спецслужб

- Падение уровня прибыльности и рост рисков, традиционных киберпреступлений
- Промышленные предприятия более уязвимыми перед угрозой кибератак по сравнению с традиционными жертвами киберпреступников
- Спецслужбы многих стран участвуют в реализации шпионских и террористических атак

3 Недооценка общего уровня угрозы

- Недостаток общедоступной информации
- Редкость целевых атак на АСУ ТП
- Излишняя вера в системы противоаварийной защиты
- Неприятие объективной реальности

4

Неправильное понимание специфики угроз и неоптимальный выбор средств защиты

- Несколько целевых атак на ограниченное количество жертв создали информационное поле, сформировавшее представление о потенциальной угрозе
- Производители средств защиты АСУ ТП создали продукты защищающие от синтетических сценариев, а не от реальных повседневных атак

5 Технические и организационные сложности защиты АСУ ТП

Неправильной оценкой текущей ситуации обусловлены следующие проблемы:

- Выполнение требований тотальной сертификации / аттестации всех средств защиты производителями средств АСУ ТП
- Выполнение требований пассивного характера работы средств защиты (работы только в режиме мониторинга)

Каракулин Сергей
Sergey.Karakulin@kaspersky.com

KASPERSKY lab