Особенности сетевой защиты АСУ ТП

Москва, 2016 г.

АСУ ТП в наши дни

В наши дни АСУ ТП используются повсеместно. Объекты, которыми управляют компьютерные системы, зачастую создают риски для окружающей среды и людей.

АСУ ТП в наши дни

- химическое производство;
- газовая и нефтяная промышленность;
- медицинские устройства;
- железнодорожный, автомобильный, авиационный транспорт и т.д.



АСУ ТП:
Возможности злоумышленника

«Никогда не было, и вот снова!»

- Средство кибератаки: неизвестно.
- Жертва: США.
- Цель атаки: Промышленный шпионаж, кража инновационных разработок.
- Итог: По некоторым оценкам США ежегодно теряют $5 триллионов или 30% своего ВВП, если учесть полную стоимость украденных инноваций

F-35 — истребитель ВВС США, на основе которого китайские военные разработали свой J-29, получив информацию через взлом государственных систем США. Фото:LockheedMartin / МэттShort. Стоимость разработки и производства $391,2 млрд.

«И один в поле воин»

- **Win32/Stuxnet** — компьютерный червь, поражающий компьютеры под управлением операционной системы Microsoft Windows. Вирус был обнаружен не только на компьютерах рядовых пользователей, но и в промышленных системах, управляющих автоматизированными производственными процессами.

«И один в поле воин»

- Червь может быть использован в качестве средства несанкционированного сбора данных (шпионажа) и диверсий в АСУ ТП промышленных предприятий, электростанций, аэропортов и т. п.

«Возвращение BlackEnergy»

- Средство кибератаки: Троян BlackEnergy.
- Жертва: Страна Украина, «Прикарпатьеоблэнерго».
- Дата: 23 декабря 2015 года.
- Цель атаки: Отключить энергоснабжение западных областей страны.
- Итог: Отключение электричества в 700 тысячах домов, пострадавшие 230 тысяч человек, сопутствующий ущерб неизвестен.

«Будни немецких сталеваров»

- Средство кибератаки: Остались неизвестны.
- Жертва: Страна Германия, сталелитейное производство.
- Дата: 2014 год.
- Цель атаки: Неизвестна.
- Итог: Физическое уничтожение доменной печи.
- Ущерб: Засекречен (стоимость современной доменной печи может составлять 170.000.000$).

Особенность защиты АСУ ТП: Критичность

Из выше изложенного можно сделать вывод, что компьютерные системы управления жизненно важными объектами должны выполнять функции безопасности и быть способны противостоять управляющим, по средствам хакерских атак, воздействиям.

Особенность защиты АСУ ТП: Выход есть

Чтобы обезопасить себя, окружающую среду и общество от разрушающих последствий атак необходимы решения, которые:

- Адаптированы к сложным производственным условиям (высокий температурный диапазон, поглощение вибрации, защита от влажности и прочее).
- Имеют централизованное управление.
- Используют промышленные протоколы.
- Имеют высокую скорость шифрования и большую пропускную способность межсетевого экрана.

Особенность защиты АСУ ТП: Выход есть

- С реализацией IPS.
- Соответствуют требованиям регуляторов (ФСТЭК России, ФСБ):
- «Требования к межсетевым экранам» (ФСТЭК России, 2016г.)
- «Требования к средствам обнаружения вторжений» (ФСТЭК России, 2013г.)
- Приказа №31 от 14.03.2014г.

Спасибо за внимание!