Изданию Financial Times Deutschland в кулуарах Мюнхенской конференции по безопасности удалось взять большое интервью у основателя Kaspersky Lab Евгения Касперского.

Касперский определил кибервойну как действия, в результате которых инфраструктура, важная для страны, подвергается манипуляциям с помощью вредных программ и в результате перестает работать. Речь, по его словам, может идти об остановке электростанций или производств вплоть до их физического разрушения. "Я думаю, что это технически возможно, потому что промышленные IT-системы должны постоянно адаптироваться и улучшаться. Это значит, что они постоянно выходят на связь с другими компьютерами или, еще хуже, постоянно подключены к интернету", - сказал он.

По словам Касперского, атака может быть проведена через программируемые логические контроллеры (PLC), с помощью которых осуществляется управление промышленными машинами. Первым подтвержденным случаем такого нападения был, по его словам, вирус Stuxnet. При этом кибероружие "гораздо дешевле обычного, и его практически невозможно обнаружить. При любом другом нападении хоть что-то можно заметить, например выдвижение войск или передислокацию боевых систем, с кибероружием иначе: что-то замечаешь только тогда, когда уже все произошло", - говорит он.

"Если мы хотим эффективно бороться с киберпреступниками, нам нужна международная киберполиция. Государства должны закрепить в соответствующем соглашении, что они будут сотрудничать при поиске преступников и террористов в интернете или кибероружия. Только так можно будет понять, действительно ли страна совершила нападение или ее компьютеры были использованы для этого третьими лицами", - говорит Касперский.

По его словам, политики уже начали понимать, что такое киберпреступность. "Они наконец говорят о сотрудничестве и о международной киберполиции. Несколько дней назад мне в Интерполе рассказали, что в 2014 году в Сингапуре откроется интернет-филиал Интерпола. Но это ограничивается киберпреступностью. Если речь заходит о кибервойне, то пока что редко встречается сознательное отношение и тем

более сотрудничество", - говорит он. При этом специалист предупреждает, что для кибероружия наиболее уязвимы развитые страны, в которых все управляется компьютерами. Разрабатывая кибероружие, они сами себе роют могилу, говорит Касперский.

По его словам, защита от кибероружия невозможна, "но пока что это понимают очень немногие. В их числе министр обороны США Леон Панетта, он недавно признался: "Мы можем нападать, но не можем защищаться", - сообщает Касперский.

Контролировать соответствующее развитие, по его словам, крайне сложно. "В конце концов, нужны только инженеры, никаких запчастей, обогащения или других сложных процессов. Разработчики ПО могут даже не осознавать, что работают над созданием оружия, если разработку оружия разделить на отдельные элементы", - говорит он.

Регламентирование для предотвращения создания подобного оружия и улучшения защиты от него, по мнению Касперского, должно включать в себя разделение интернета на различные зоны. "Обычный гражданин может жить в Сети как хочет. Но тот, у кого есть доступ к критичной инфраструктуре, должен принять строгие правила и не делать определенных вещей", - говорит он, упоминая, в том числе, ведение блога и оставление комментариев в других блогах. "На самом деле, это существует даже сейчас: например, уже теперь у президентов нет мобильных телефонов", - замечает он.

По словам Касперского, самой легкой жертвой кибератак на данный момент могут стать Соединенные Штаты, поскольку это наиболее развитая с точки зрения информационных технологий страна, имеющая массу выходов в интернет.

Предприятия в состоянии защитить свою безопасность, отделив особенно важные части IT-системы от Сети, говорит он. "Можно применять только избранные, заранее разрешенные программы. А работники должны иметь доступ только к тем данным и приложениям, которые нужны им для работы", - советует Касперский.

Редакция
Financial Times Deutschland
Источник материала: InoPressa.ru