Инструкция по противодействию вредоносному программному обеспечению

ФСБ России выявлены факты систематической рассылки вредоносного программного обеспечения (далее - ВПО) по каналу электронной почты в адрес органов государственной власти, предприятий ОПК и объектов жизнеобеспечения Российской Федерации.

ВПО имеет отдельные признаки программных средств скрытого информационного воздействия, содержится во вложениях электронных писем, направляемых зарубежной стороной от имени легальных предприятий и организаций под предлогом предоставления сведений, содержащихся в прикрепленных файлах, как правило, упакованных в архив.

Обращаю внимание, что при работе с вложениями электронных писем необходимо:

1. Оценить легальность отправителя электронного письма (адрес электронной почты, с которой поступило сообщение).
2. Не открывать и не скачивать вложения с расширениями exe, bat, cpl, dll, jar, msi, scr).
3. Вложения с расширениями rar или zip (архивы) скачивать и открывать только при подтверждении легальности отправителя.
4. Любое скачиваемое вложение перед открытием проверять антивирусной программой. При обнаружении вирусов незамедлительно, файл открывать запрещается, незамедлительно сообщить специалисту по ТЗИ Минтруда.
5. Если вложение – файл программ офисного пакета Microsoft Office и при открытии файла запрашивается разрешение на выполнение макроса, необходимо запретить выполнение макроса, зарыть программу, незамедлительно сообщить специалисту по ТЗИ Минтруда.
6. При невозможности оценить легальность отправителя – незамедлительно обращаться к сотрудникам отдела информационных технологий и защиты информации Министерства.
7. При возникновении любой нетипичной ситуации в работе объекта вычислительной техники (инцидента) - незамедлительно обращаться к сотрудникам отдела информационных технологий и защиты информации Министерства