Памятка пользователям о мерах противодействия вредоносному программному обеспечению (ВПО)

Самым распространённым способом доставки вредоносного программного обеспечения до пользователей является отправка по электронной почте вложенного файла, содержащего вредоносный код. Для заражения компьютера **требуется, чтобы пользователь открыл указанный файл**. Злоумышленники используют различные ухищрения для того, чтобы побудить пользователя открыл файл: разрабатывают специальные тексты писем, пишут их от имени органов государственной власти и государственных организаций, в том числе контрольно-надзорных органов, предлагают товары (услуги) по особым ценам, информируют об имеющейся задолженности, о направлении актов сверки и иных финансовых документов, сообщают о попавших в беду близких или пишут от их имени и т.п.

С целью сведения к нулю риска проникновения ВПО в рабочий ПК необходимо соблюдение пользователем ряда несложных правил:

1. Если Вы получили письмо с вложенным файлом, нельзя сразу открывать его! Прежде чем это делать, убедитесь в надёжности источника и безопасности вложения.

2. Обратите внимание на адрес и подпись отправителя. Если адрес явно не соответствует подписи (например, письмо с адреса ivanov@nalog.ru, а в подписи написано Петров Пётр Петрович) – это наверняка письмо с ВПО.

3. Если это известный Вам человек – уточните у него, действительно ли он направил Вам письмо с вложенным файлом, и если не отправлял – не открывая вложения, сообщите о получении такого письма ответственному за информационную безопасность в ИОГВ или администраторам ИВС ИОГВ.

4. Если отправитель Вам неизвестен, но содержание письма представляет интерес, не открывая файл, напишите ответ (с помощью кнопки «Ответить») адресату и задайте ему любой уточняющий вопрос. Если это письмо от злоумышленников – ответа Вы скорее всего не получите, возможно, и Ваше письмо вернётся с пометкой «не удаётся доставить», либо с Вами свяжется отправитель письма, который с недоумением сообщит, что он Вам ничего не отправлял. Также Вы можете попробовать связаться с отправителем письма по представленным им контактным данным и уточнить у него информацию об отправке письма и содержании вложений.
Отсутствие в письме контактной информации – один из признаков того, что это письмо от злоумышленников. Настоящий сотрудник государственного органа или организации-контрагента не заинтересован скрывать контактную информацию.

5. При любых сомнениях в безопасности вложенного файла, даже если Вы убедились в надёжности источника – не открывайте его, сообщите о своих сомнениях ответственному за информационную безопасность в ИОГВ или администраторам ИВС ИОГВ.

6. **Не открывайте на рабочем ПК файлы, полученные по электронной почте на личные адреса с использованием веб-интерфейса, даже если это необходимо в служебных целях, если у Вас нет уверенности в их безопасности**. Сделайте это на личном компьютере, если Вы полагаете, что информация может представлять интерес, или выполните пересылку себе на рабочий адрес электронной почты. Если при пересылке письмо пришло без вложения или не пришло вообще – скорее всего письмо содержало ВПО.

На почтовом сервере ИВС ИОГВ установлено современное и актуальное программное обеспечение, работа которого направлена на противодействие рассылкам нежелательной корреспонденции (спама) и поиску и обезвреживанию ВПО. Зачастую злоумышленники используют именно различные механизмы рассылки спама для распространения своего вредоносного программного кода.
Ежедневно этим программным обеспечением блокируется порядка 50 000 (пятидесяти тысяч) писем, поступающих в адрес пользователей ИВС ИОГВ (адреса электронной почты в домене @gov-murman.ru), среди которых как нежелательная реклама, так и вредоносные программы, которые могут выполнять различные функции: хищение данных пользователя («фишинг»), попытка передать отправителю ВПО удалённое управление АРМ пользователя («троян»), шифрование данных пользователя для последующего вымогания денежных средств за расшифровку («шифратор»).
Вместе с тем, как показывает практика, новые вредоносные программы и новые механизмы рассылки спама появляются на некоторое время (несколько часов или дней) быстрее, чем механизмы, позволяющие с ними бороться.
Поэтому полностью полагаться только на автоматические фильтры нельзя. В редких случаях полезные письма от организаций-контрагентов могут не доходить до получателей – пользователей ИВС ИОГВ – в связи с работой автоматических фильтров. О таких случаях необходимо сообщать администраторам ИВС ИОГВ.

Просим не терять бдительность и внимательно относиться ко всем сообщениям с вложениями, которые поступают Вам по электронной почте.