**Дополнительные меры по обеспечению информационной безопасности при работе с электронной почтой:**

1. Внимательно проверять адрес отправителя даже в случае совпадения имени с уже известным контактом.
2. Не открывать письма от неизвестных адресатов.
3. Проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку.
4. Не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или, наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т.д.).
5. Не нажимать на ссылки из письма, если они заменены на слова, не наводить на них курсор.
6. Проверять ссылки, даже если письмо получено от другого пользователя информационной системы.
7. Не открывать вложения, особенно если в них содержаться документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD.
8. Внимательно относиться к письмам на иностранном языке с большим количеством получателей.