**Рекомендации по противодействию программным средствам скрытого информационного воздействия (далее - ПССИВ) при обработке электронных почтовых сообщений**:

1. Использовать на всех объектах информационно­телекоммуникационной сети (далее - ИТС) сертифицированные ФСБ России антивирусные средства с актуальными антивирусными базами.
2. В антивирусных средствах объектов ИТС настроить периодическую (не реже 1 раза в неделю) полную проверку системных и пользовательских каталогов операционной системы (далее - ОС), а также полную (не реже 1 раза в месяц) проверку всех несъемных носителей информации.
3. Настроить в антивирусных средствах объектов ИТС процедуру принудительной проверки подключаемых внешних носителей информации.
4. Организовать на сервере электронной почты антивирусную проверку всех входящих писем и периодическую проверку накопленной электронной корреспонденции.
5. Организовать на сервере электронной почты фильтрацию входящей электронной корреспонденции на предмет наличия спам сообщений, а также электронных писем, содержащих во вложении исполняемые файлы (EXE, ВАТ, CPL, DLL, JAR, MSI, SCRи т.д.).
6. Организовать просмотр вложений электронных писем, поступающих на публичный (опубликованный в сети Интернет) почтовый адрес организации, на выделенном средстве вычислительной техники (далее - СВТ) с установленной на нем ОС семейства Linuxи свободно распространяемым пакетом офисных программ. Целью указанных мероприятий является проверка вложенных электронных документов на предмет наличия ПССИВ, признаком которых может являться появление сообщений об ошибках в работе офисных программ при открытии вложенных электронных документов. В случае появления указанных сообщений об ошибках рекомендуется удалять электронные письма, содержащие вложения, предположительно зараженные ПССИВ, и не открывать указанные вложения на других СВТ.
7. Организовать антивирусную проверку входящего веб-трафика.
8. Организовать фильтрацию входящего веб-трафика с использованием контент-фильтров (сайтов развлекательного характера и сайтов социальных сетей, запрет посещения потенциально опасных сайтов, запрет загрузки исполняемых файлов).
9. Своевременно устанавливать критические обновления безопасности для прикладного программного обеспечения, в том числе офисных пакетов, средств просмотра PDF документов, интернет-браузеров, средств работы с Flash и Java приложениями.
10. Отключить в настройках офисных программ возможность работы с макросами.
11. Осуществить настройку системы разграничения прав доступа ОС с целью предоставления пользователям минимально необходимого перечня прав доступа (ограничить возможность установки программного обеспечения, создания файлов в системных директориях, запуска исполняемых файлов из пользовательских каталогов).