Приложение №2 к Письму
Министерства цифрового развития
и связи Кузбасса
от _____ № _____

Рекомендации по использованию почты, настройке почтовых клиентов

В соответствии с письмом Управления ФСТЭК России по Сибирскому федеральному округу от 11.02.2025 № 387 с целью предотвращения реализации угроз безопасности информации, связанных с деятельностью хакерских группировок, а также для недопущения утечки конфиденциальной информации, в том числе персональных данных, необходимо реализовать дополнительные меры защиты:

1.1. Производить проверку почтовых вложений с использованием средств антивирусной защиты:

для антивирусного средства Kaspersky Endpoint Security необходимо использовать функцию «Защита от почтовых угроз». Для того, чтобы включить указанную функцию, необходимо перейти в настройки приложения и в разделе «Базовая защита» активировать функцию «Защита от почтовых угроз»;

для антивирусного средства Dr.Web Security Space необходимо использовать утилиту SpIDer Mail. Для того, чтобы задействовать указанную утилиту необходимо перейти в настройки приложения и в разделе «Компоненты защиты» выбрать и активировать утилиту SpIDer Mail.

1.2. Проверять имя домена отправителя электронного письма в целях идентификации отправителя. Для этого необходимо обращать внимание на наименование почтового адреса (домена), указанного после символа «@», и сопоставлять его с адресами (доменами) органов (организаций), с которыми осуществляется служебная переписка. Особое внимание уделить фейковым почтовым адресам, содержащим упоминание контролирующих органов (например ФСБ России – fsb.rf_list.gov@mail.ru, fsb_rf_fsb@mail.ru).

1.3. Организовать получение почтовых вложений только от известных отправителей. Для этого необходимо организовать ведение списков адресов электронной почты органов (организаций), с которыми осуществляется взаимодействие. Почтовые адреса контролирующих, координационных и иных органов, с кем осуществляется взаимодействие, необходимо проверять через их официальные сайты, например: http://nac.gov.ru/ ; http://www.fsb.ru/ ; https://fstec.ru/.

1.4. Не открывать и не загружать почтовые вложения писем с тематикой, не относящейся к деятельности органа (организации).

1.5. Осуществлять работу с электронной почтой под учетными записями пользователей операционной системы с минимальными возможными привилегиями:

для операционных систем семейства Microsoft Windows ограничение привилегий можно осуществить через «Панель управления» - «Учетные записи пользователей» - «Управление учетными записями»; для операционных систем семейства Linux возможно использование команд chmod, chown, chgrp для разграничения прав доступа к файлам и директориям как отдельных пользователей, так и групп пользователей.