Рекомендации сотрудникам, преподавателям и обучающимся по защите информации при работе в удаленном формате

В целях минимизации рисков возникновения угроз безопасности информации при осуществлении удаленного режима работы соблюдать требования по защите информации, прежде всего:

- исключить доступ посторонних лиц к компьютерам на рабочих местах, при оставлении рабочего места блокировать компьютер. В случае, если компьютер используется несколькими пользователями (преподаватели, сотрудники, обучающиеся), при оставлении рабочего места выполнять выход из аккаунтов электронной почты, информационных систем, используемых сервисов и т.п.;
- использовать сложные пароли (не менее 6-8 символов, с использованием букв, цифр и спецсимволов) для входа в операционную систему компьютера и сервисы университета, менять их не реже 1 раза месяц;
- всегда использовать антивирусное программное обеспечение на компьютере в режиме фоновой защиты, следить за актуальностью антивирусных баз. Съемные носители информации перед использованием проверять на вирусы;
- использовать для работы на средствах вычислительной техники (ПЭВМ, мобильные электронные устройства) учетные записи операционных систем и сервисов с ограниченными правами (без прав администратора с полным доступом к системе);
- не устанавливать программное обеспечение из сомнительных источников. Использовать программное обеспечение только необходимое для работы;
- использовать для документооборота только корпоративную почту и сервисы СФУ;
- быть внимательными при получении входящих электронных сообщений: не открывать подозрительные и неизвестные входящие электронные сообщения, не переходить по ссылкам в почтовых сообщениях, в которых сообщается о необходимости обновления учетных данных, увеличения лимитов электронной почты, «активации своего профиля» или его «продления». Подобные письма являются мошенническими и их целью является получение злоумышленниками корпоративных учетных данных пользователя: логина и пароля и других противоправных действий. Администрация университета и ИТ-службы никогда не рассылают подобных писем;
- не использовать публичные облачные хранилища для хранения рабочих документов;
- соблюдать требования к информационной безопасности при работе в интернете: не скачивать и не запускать незнакомые файлы, не посещать подозрительные ресурсы, сайты, не вводить на них логины и пароли;
- сводить к минимуму передачу информации, особенно персональных данных, при электронном документообороте, не сообщать данные паспортов РФ, зачетных книжек и других документов.