Памятка по информационной безопасности при работе с конфиденциальными сведениями

1) Информация ограниченного доступа (в том числе с ограничительной пометкой «Для служебного пользования»), не содержащая сведений, составляющих государственную тайну, должна обрабатываться в электронном виде только на рабочих местах, аттестованных по требованиям безопасности информации, предъявляемым ФСТЭК России к таким автоматизированным рабочим местам.

2) Информация, содержащая сведения составляющие государственную тайну, должна обрабатываться в электронном виде только на рабочих местах, аттестованных по требованиям безопасности информации, предъявляемым ФСТЭК России и ФСБ России к таким автоматизированным рабочим местам.

3) Провести детальный анализ адресов электронной почты, созданных на сторонних почтовых сервисах (mail.ru, yandex.ru, rambler.ru, google.com и др.) в подконтрольных Вам структурных подразделениях на предмет их использования в служебных целях.

4) Запретить использование личных адресов электронной почты в рабочих целях.

5) Провести дополнительные настройки корпоративной электронной почты и почтовых серверов, при наличии, для обеспечения ее безопасности: включение двухфакторной аутентификации с использованием доверенного номера телефона, установка контрольных вопросов, включение уведомлений о новых устройствах, с которых выполнен вход в электронную почту.

6) Актуализировать необходимое количество сотрудников, которым необходим доступ к групповым адресам электронной почты Управлений, Комитетов или отделов. Определить список работников, имеющих доступ к электронной почте, и строго соблюдать конфиденциальность обрабатываемой информации, а также актуальность списка работников. Особое внимание уделить смене парольных комбинаций при проведении организационно-штатных мероприятий (увольнения, переводы и др.)

7) Обеспечить смену пароля на используемых адресах электронной почты не реже, чем раз в три месяца. Пароль должен отвечать требованиям по информационной безопасности и быть устойчивым к взлому (длина пароля не менее 8 символов, пароль должен содержать прописные и строчные буквы, цифры (не менее двух) и специальные символы !@#$%^&*() (например: 29Akf<ezPfg, Qu88nC@rd13). Не использовать одинаковые пароли к разным информационным ресурсам.

8) Запрещено сохранять пароли в браузере, а также хранить их в рукописном виде в легкодоступных местах (стикеры на рабочих столах). Рекомендуемые

способы хранения паролей – менеджеры паролей, запись в личном блокноте, исключающая ознакомление других лиц.

9) На рабочих местах должно быть установлено средство антивирусной защиты. При уходе работника из кабинета, необходимо блокировать паролем рабочее место.

10) Исключить переписку по электронной почте и интернет-мессенджерам по тематикам оперативного штаба по обеспечению кибербезопасности, Антитеррористической комиссии Челябинской области и оборонными предприятиями, а также с иными владельцами чувствительной информации, утечка которой может нанести ущерб безопасности.

11) Необходимо назначить работника, ответственного за обеспечение информационной безопасности. В его должностные обязанности должно входить информирование коллег об угрозах информационной безопасности, проведение инструктажей по вопросам обеспечения информационной безопасности, а также проводить аудит информационной сети организации на предмет реализации угроз.