Инструкция по использованию
персональных мобильных устройств в рабочих целях

1. Устройства

1.1. Строго не рекомендуется:

использовать для рабочих коммуникаций мобильные устройства корпорации Apple;

использовать носимые, в том числе «умные» устройства (умные часы, фитнес-браслеты и т.п.) во время работы, так как они могут передавать в сервисы сбора данных («облако») биометрические данные: пульс, нагрузку, количество шагов вместе с географическим положением, номерами телефонов, логами звонков, именами сетей Wi-Fi и другой личной информацией;

разрешать приложениям выводить сообщения на экран блокировки мобильного устройства;

использовать или держать включёнными мобильное устройство на совещаниях и переговорах;

оставлять видимым мобильное устройство через технологию Bluetooth, кроме моментов сопряжения с «известными» устройствами;

использовать сервис геопозиционирования мобильного устройства (GPS) на территориях, где возможно проведение контртеррористических и иных специальных операций, а также за исключением времени его практического использования.

1.2. Рекомендуется использование для рабочих целей отдельного мобильного устройства, функционирующего на российской операционной системе (Аврора), либо на операционной системе Android с учетом отсутствия на нем установленных личных и развлекательных приложений (рекомендованные производители:

российские – Aquarius, AYYA;

южнокорейские – Samsung;

китайские – Xiaomi, OnePlus, Honor, Meizu и др.).

2. Сервисы коммуникаций (текстовые сообщения, аудиозвонки, отправка файлов)

2.1. Запрещается использование мессенджеров WhatsApp и Viber.

2.2. В личных целях рекомендуется использование мессенджеров VK Мессенджер, eXpress, Telegram (секретные чаты), Signal.

2.3. Для конфиденциальных разговоров (в том числе при общении с новыми регионами) рекомендуется использовать сервис ViPNet Connect.

Для получения учетных данных и начала работы с сервисом ViPNet Connect необходимо руководствоваться инструкцией:

https://mes.cism-ms.ru/vipnet_connect_howto.pdf

3. Антивирусная защита

3.1. Любые скачанные приложения, в том числе с известных «контактов» в виде файлов, интернет-ссылок, писем и сообщений необходимо проверять средствами антивирусной защиты (встроенной в функционал мобильного устройства проверки пакетов недостаточно). Для этих целей рекомендуется использование российских антивирусных средств: Kaspersky Internet Security – https://play.google.com/store/apps/details?id=com.kms.free, Dr.Web – https://play.google.com/store/apps/details?id=com.drweb.

3.2. Строго рекомендуется проводить принудительную полную антивирусную проверку мобильного устройства не реже 1 раза в месяц, а также незамедлительно при подозрении на его нештатную работу (замедление работы, подозрительная активность одного или нескольких установленных приложений).

4. Аутентификация

4.1. Строго не рекомендуется:

использовать в качестве основного средства защиты от несанкционированного доступа к мобильному устройству пин-код и графический ключ, поскольку данный способ считается небезопасным.

использовать одинаковые пароли для различных ресурсов.

4.2. Рекомендуется:

использовать в качестве основного средства защиты от несанкционированного доступа к мобильному устройству текстовый пароль или биометрические средства аутентификации;

активировать в используемых программах двухэтапную аутентификацию (SMS/push и пароль).

5. Социальные сети

5.1. Запрещено ведение служебной переписки, опубликование и распространение любой информации (медиаданных), касающихся рабочих вопросов, посредством социальных сетей.

5.2. В целях недопущения информационных утечек и атак строго не рекомендуется опубликование и распространение посредством социальных сетей любой информации (медиаданных), касающихся личных данных, в том числе в принадлежащих родственникам аккаунтах.

6. Нахождение на территориях Донецкой Народной республики, Луганской Народной республики, Херсонской и Запорожской областей

6.1. Запрещено иметь при себе включенное мобильное устройство вблизи границы и линии боевого соприкосновения.

6.2. В настройках телефона, касающихся определения оператора связи, необходимо установить вручную выбор оператора связи, чья SIM-карта была приобретена (базовые станции других государств могут распространять сигнал на расстояния более 30 км).