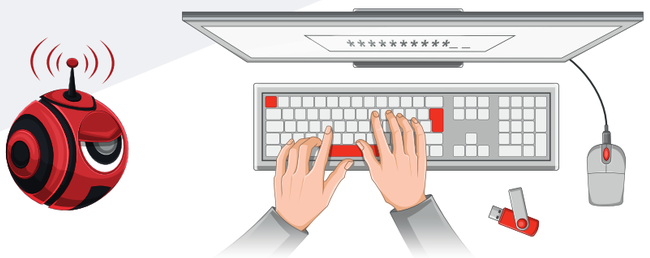
ПАМЯТКА ПО ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЗНАЙ И СОБЛЮДАЙ!

1 ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ НА ПК

- Минимизировать работу с внешними источниками информации на рабочем ПК, на котором обрабатывается служебная информация
- Исключить возможность ознакомления третьих лиц со служебной информацией (например, визуально с экрана монитора или путем его фотографирования)
- Обязательно проверять на вирусы любой съемный носитель информации при его подключении к ПК
- **НЕ загружать и НЕ открывать служебные файлы (документы) на личных ПК**
- **НЕ подключать к рабочему ПК USB-модем и мобильные устройства (смартфон, планшет и т.п.)**



2 ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЦИФРОВЫХ КОММУНИКАЦИЯХ

- Использовать для обмена служебной информацией **(за исключением информации конфиденциального характера!)** только корпоративные сервисы информационно-телекоммуникационных сетей: для мгновенного обмена сообщениями – ЕКС МОС на базе мессенджера eXpress; для обмена файлами большого объема – КСОФ на базе Mflash
- Использовать служебную электронную почту только для выполнения производственных задач
- Проверять все файлы, поступившие из электронной почты и социальных сетей, на вирусы перед тем, как открывать их
- **НЕ использовать для обмена служебной информацией мобильные технические средства производства компании «Apple»**
- **НЕ размещать информацию служебного характера в открытых источниках (социальные сети, форумы, сетевые диски, электронная почта в сети Интернет, облачные хранилища и т.п.)**
- **НЕ публиковать в социальных сетях в качестве обратной связи адреса корпоративной электронной почты**
- **НЕ публиковать в социальных сетях фотографии личных документов (паспорт, водительские права, служебное удостоверение, служебный пропуск)**

3 ЗАЩИТА ОТ ФИШИНГА В СЕТИ ИНТЕРНЕТ

- Обращать внимание на название сайтов, на которых вводятся учетные данные (логин, пароль, пин-код), даже в случае визуального совпадения с уже известным сайтом
- Внимательно проверять адрес отправителя, даже в случае визуального совпадения имени с уже известным контактом
- Проверять ссылки в сообщениях, даже если письмо получено от коллеги. Нужно помнить, что электронную почту коллеги или знакомого могли взломать
- Рекомендуем подозрительно относиться к письмам с призывом к действиям (например «открой», «прочитай», «ознакомься»), с темами про финансы, банки, геополитическую обстановку или угрозы

4 ЦИФРОВОЙ СЛЕД

- **ЗАПРЕЩАЕТСЯ** использовать для пересылки служебной информации любые сервисы информационно телекоммуникационных сетей иностранного производства (включая электронные почтовые сервисы, файловые и облачные хранилища, сервисы обмена сообщениями, сервисы делового планирования, мессенджеры):

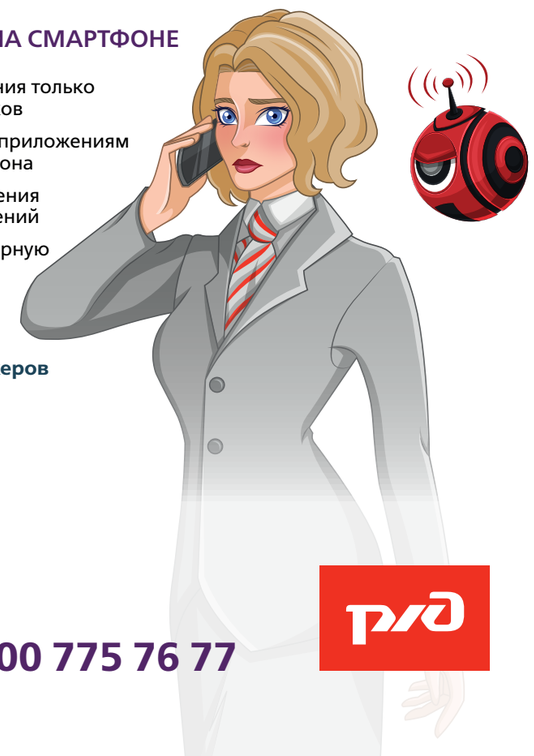
  Gmail.com; Icloud.com; Google Drive; WhatsApp; Telegram; Skype; Viber; Zoom; Facebook Messenger и другие…

5 ТРЕБОВАНИЯ К ПАРОЛЬНОЙ ЗАЩИТЕ

- Использовать надежные пароли на своих устройствах (ПК, роутеры и др.): не менее 12 символов, содержащих прописные и строчные буквы (a-z, A-Z), цифры и спец. символы (&*!% и т.п.). Сверять со списками Топ-популярных паролей, публикуемых в открытых источниках
- Создавать уникальные пароли для каждого устройства и сервиса (для социальных сетей, личной электронной почты, служебных программ)
- Использовать двухфакторную аутентификацию там, где это предусмотрено системой (подтверждение действий пользователя по электронной почте, SMS)
- Регулярно менять пароли на устройствах (раз в 3 месяца), не использовать их повторно
- **НЕ сохранять пароли в программах или браузере (автозаполнение)**
- **НЕ передавать логины и пароли от своих учетных записей в информационных системах ОАО «РЖД» третьим лицам, в том числе работникам ОАО «РЖД»**
- **НЕ хранить пароли в электронной почте, а также на бумажных носителях информации в общедоступных местах (например, на столе или под клавиатурой и т.п.)**

6 ЗАЩИТА ДАННЫХ НА СМАРТФОНЕ

- Устанавливать приложения только от доверенных источников
- Осмысленно разрешать приложениям доступ к ресурсам телефона
- Включить push-уведомления для банковских приложений
- Использовать двухфакторную аутентификацию
- **НЕ переходить по подозрительным ссылкам из СМС, календарей, мессенджеров**



Горячая линия для работников ОАО «РЖД» по вопросам информационной безопасности 8 800 775 76 77