ПАМЯТКА
пользователя АРМ по обеспечению информационной безопасности

Работа на АРМ

- Не допускайте других лиц для работы на своем компьютере.
- Обеспечьте сохранность ключевого носителя (USB-ключ, смарткарта):
  - в личном сейфе / металлическом шкафу;
  - в сейфе / металлическом шкафу коллективного пользования в опечатанных конвертах, тубусах;
  - при себе, если при этом обеспечивается надёжный контроль доступа к носителю со стороны владельца ЭП.
- Никому не передавайте свои ключевые носители.
- Не сообщайте никому своих паролей и пин-кодов (в том числе коллегам, лицам, обслуживающим АРМ, руководителям). Не храните записанные пароли и пин-коды в общедоступных местах.
- Блокируйте экран компьютера при уходе с рабочего места.
- Используйте пароль, содержащий не менее 8 символов, буквы различного регистра, цифры и спецсимволы.
- Используйте только свои учетные записи и ключевые носители.
- Используйте сетевые каталоги для хранения файлов, содержащих корпоративно-значимую информацию.
- Не запускайте на АРМ файлы, полученные из неизвестных или из не заслуживающих доверие источников, или сторонние программы.
- Не храните на жёстких дисках АРМ и сетевых папках личную информацию и информацию, не относящуюся к производственной деятельности или исполнению должностных обязанностей.
- Не вскрывайте системные блоки компьютеров, не изменяйте штатную конфигурацию АРМ, не подключайте нештатные устройства (клавиатура/мышь, устройства связи, модемы и пр.).
- Располагайте мониторы и печатающие устройства таким образом, чтобы исключить несанкционированный доступ других лиц к отображаемой и выводимой на печать информации. Не оставляйте документы в принтере или в сканере.
- Не покидайте рабочее место, если кто-то проводит работы на Вашем АРМ.
- Не фотографируйте документы с конфиденциальной информацией, экраны компьютеров и не осуществляйте их аудио- и видеозапись.

Работа в сети Интернет

- Не обсуждайте, не передавайте конфиденциальную информацию в интернет-мессенджерах.
- Не передавайте в сеть Интернет (файлообменные сервисы) конфиденциальную информацию, в том числе ПД, без применения средств криптографической защиты информации.
- Не посещайте сомнительные интернет-сайты, не скачивайте с них и не запускайте на АРМ какие-либо файлы.
- Минимизируйте загрузку файлов из сети Интернет.
- Не оставляйте без необходимости на сайтах в сети Интернет персональные данные (ФИО, должность, телефоны, e-mail и пр).
- Не сохраняйте в браузере ваши пароли для доступа к сайтам в сети Интернет.
- ПОМНИТЕ, ЧТО РАБОТА С ИНТЕРНЕТ-СЕРВИСАМИ (социальные сети, почтовые и файлообменные сервисы, online-переводчики и пр.) СОЗДАЕТ ПРЕДПОСЫЛКИ ДЛЯ УТЕЧКИ ИНФОРМАЦИИ.

Работа с электронной почтой

- Не открывайте вложения, не переходите по ссылкам, не открывайте файлы и не запускайте программы, полученные по электронной почте от неизвестного Вам отправителя или из писем, контекст переписки в которых не соответствует ожидаемому.
- Не отправляйте конфиденциальную информацию, в том числе персональные данные (ПД), без применения средств исключающих несанкционированное ознакомление с информацией лиц к ней не допущенных.
- Максимально ограничьте отправку информации, относящейся к производственной деятельности Общества, на бесплатные почтовые серверы. При необходимости отправки применяйте шифрование файлов средствами криптографической защиты информации.
- Не отправляйте ПД работников Общества (иных субъектов ПД) на личную почту.
- Передавайте получателю электронного письма служебную и производственную информацию в объеме минимально необходимом для решения производственных задач.
- Не используйте служебные почтовые адреса для целей, не связанных с производственной деятельностью, в том числе не указывайте адрес электронной почты при регистрации на сайтах в сети Интернет.
- Перед отправкой сообщения внимательно проверяйте адреса получателей в целях предотвращения передачи информации третьим лицам.

Работа с внешними носителями данных

- Минимизируйте хранение информации, относящейся к производственной деятельности Общества, на внешних носителях данных.
- Отключайте внешние носители данных от компьютера по окончании использования.
- Обеспечьте хранение внешних носителей данных с соблюдением условий, исключающих несанкционированный доступ к ним.
- Не допускайте хранение и обработку конфиденциальной информации, в том числе ПД, на не учтенных установленным порядком внешних носителях данных.
- Без наличия служебной необходимости не подключайте к АРМ в качестве внешних носителей данных нештатные устройства (фотоаппараты, телефоны, смартфоны, планшеты и др.).
- Храните документы с конфиденциальной информацией в запираемых шкафах, ящиках, сейфах.
- Уничтожайте ненужные бумажные документы с помощью шредера (кроме документов, полученных у ответственного за конфиденциальное делопроизводство).
- Не выносите документы с конфиденциальной информацией за пределы территории Общества без разрешения руководителя структурного подразделения.

Работники обязаны знать и выполнять положения и требования локальных нормативных актов и документов Общества по обеспечению режима коммерческой тайны, защите информации и персональных данных, соблюдению правил работы в информационных системах и на АРМ.