Памятка пользователю по информационной безопасности

Парольная защита

• Никогда не сохраняйте ваши пароли в программах. Большинство программ хранят их в открытом виде и тот, кто получит доступ к вашему компьютеру, получит доступ и к ним.

• Сохраняйте в тайне личный пароль. Никогда не сообщайте пароль другим лицам, и не храните записанный пароль в общедоступных местах.

• В случае производственной необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, выполняемых отделом (специалистом) по защите информации, работ, проводимых отделом АСУ и требующих знания пароля пользователя, допускается раскрытие значений своего пароля начальникам этих подразделений. По окончанию производственных, или проверочных работ работники самостоятельно производят немедленную смену "раскрытых" паролей.

• Не используйте пароль доступа в локальную сеть филиала в других программах и на сайтах, где требуется регистрация;

• Следует помнить, что для печати документов на принтере, подключенном к другому компьютеру, не требуется знать пароль от этого компьютера. Достаточно включить компьютер, к которому присоединен нужный принтер. После появления приглашения можно осуществлять печать. Для выключения компьютера нужно нажать кнопку «Завершить работу» не вводя пароль.

Антивирусная защита

• Никогда не отключайте установленное на АРМ антивирусное программное обеспечение.

• Обязательно проверяйте на наличие вирусов все внешние носители информации (оптические диски, флешки и т.п.), поступающие со стороны (из внешних организаций, других подразделений Организации и т.п.).

• Во всех случаях возможного проявления действия вирусов или подозрении на наличие вируса не пытайтесь удалить вирус самостоятельно, незамедлительно сообщите об этом ответственному за антивирусный контроль и оцените с ним возможные пути заражения и распространения данного вируса.

Интернет и электронная почта

• Содержание Интернет-ресурсов, а также файлы, загружаемые из Интернета, обязательно проверяйте на отсутствие вредоносных программ и вирусов.

• Не переходите по ссылкам, не запускайте программы и не открывайте файлы, полученные по электронной почте от неизвестного Вам отправителя.

• Не передавать по электронной почте Ваши пароли.

• Не принимайте никаких соглашений при посещении сайтов, смысла которых Вы не понимаете.

Безопасность при осуществлении платежей

• По возможности, используйте дополнительное подтверждение операций, например, с помощью SMS или иным способом (например, по телефону).

• Не переходите по ссылкам, полученным от неизвестных лиц. При получении писем или сообщений от банков удостоверьтесь, что вам пишет именно банк.

• Будьте внимательны при осуществлении платежей в интернете. Проверяйте наличие https// в адресной строке браузера и точность адреса.

Прочее

• Не поднимайте и не используйте найденные на улице, или других общественных местах, носители информации.

• Не устанавливайте самостоятельно программное обеспечение, если это не входит в Ваши обязанности. Запрещается устанавливать и запускать не относящееся к выполнению Ваших должностных обязанностей программное обеспечение.

• Располагайте мониторы и печатающие устройства таким образом, чтобы исключить несанкционированный доступ к отображаемой и печатаемой информации.

• При временном оставлении рабочего места в течение рабочего дня в обязательным порядке, блокируйте компьютер нажатием комбинации клавиш «Win + L».

• Не пользуйтесь незащищенными Wi-Fi-сетями.

• С осторожностью относитесь к нестандартным сообщениям в интернете (особенно в социальных сетях). Помните, что любые нестандартные просьбы могут быть мошенничеством.

• Не используйте бесплатную почту и чаты для передачи персональной информации.

• С осторожностью относитесь к хранению информации в облаке. Следует шифровать данные для хранения их в облаке либо сделать выбор в пользу хранения информации локально.

• Не берите смартфон на важные переговоры.

• Не используйте мобильное устройство для конфиденциальной переписки.