Общество с ограниченной ответственностью «Объединенная управляющая компания»

Рекомендации клиентам и партнерам по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники

1. Программная защита

1.1. Используйте технические устройства с установленным лицензионным программным обеспечением;

1.2. Своевременно обновляйте операционную систему, особенно в части обновлений безопасности, это позволит снизить риски заражения вредоносным кодом;

1.3. На рабочем/домашнем компьютере должен быть установлен антивирус, если его нет, то незамедлительно установить его (самостоятельно или с помощью администратора системы);

1.4. Обязательное автообновление антивирусных баз. Если антивирусные базы не обновляются, очень устарели (антивирусное ПО обычно сообщает об этом спецзначками в панели задач на своей иконке), то необходимо незамедлительно обратиться за помощью к IT-специалисту. При этом ни в коем случае не отключайте антивирусную защиту;

1.5. Периодически, не реже 1 раза в месяц проводите полную проверку системы на вирусы.

2. Правила использования внешних носителей информации (USB-флеш, SD-карты)

2.1. Настройте опции антивируса на обязательную автоматическую проверку всех присоединяемых внешних (съемных) USB устройств;

2.2. Настройте опции антивируса на запрет записи на внешние носители информации.

2.3. Отключите Автозапуск на просмотр содержимого внешних носителей.

2.4. Не используйте корпоративные внешние носители информации на домашнем ПК. Так же исключите возможность подключения личных USB устройств хранения данных в корпоративных сетях.

3. Правила обмена конфиденциальной информацией

3.1. Используйте, по возможности, защищенные каналы связи, личные кабинеты ЭДО;

3.2. Если планируете передавать конфиденциальную информацию с использованием сети Интернет, то зашифруйте пакет передавайнмых данных средствами криптографической защиты (СКЗИ).

4. Правила использования электронной почты (e-mail)

4.1. Письма, приходящие по электронной почте, могут содержать вредоносные файлы или ссылки, ведущие на зараженные сайты. При открытии такого файла или переходе по ссылке вирус попадает на компьютер пользователя.

4.2. Не переходите по ссылкам из подозрительных писем;

4.3. Не открывайте письма с вложениями, полученные от неизвестных отправителей;

4.4. Не отвечайте на сообщения, требующие предоставить, подтвердить или уточнить вашу конфиденциальную информацию: пароли, логины, фамилию, имя, отчество, паспортные данные, номер мобильного телефона, на который поступают одноразовые пароли и другие данные.

5. Правила работы в сетях общего доступа и (или) международного обмена

5.1. Не используйте общественные беспроводные сети и устройства для работы с личной информацией;

5.2. Не используйте программные продукты, полученные из сомнительных источников (пиринговые и файлообменные сети), модифицированные программные продукты, не посещать ресурсы с сомнительной репутацией;

5.3. Если необходимо ввести на сайте личную информацию, то лучше использовать безопасное

соединение: в адресной строке браузера URL веб-сайта должен начинаться с «https://», в интерфейсе браузера должна появиться иконка замка).