ПРИЛОЖЕНИЕ

Рекомендации по обеспечению защищенности аккаунтов в социальных сетях

1. Общие положения

Настоящие рекомендации разработаны в соответствии с постановлением Правительства Хабаровского края от 17.03.2020 № 77-пр "О взаимодействии органов исполнительной власти Хабаровского края с населением Хабаровского края в информационно-телекоммуникационной сети "Интернет" в целях обеспечения защищенности аккаунтов в социальных сетях (далее – Аккаунты).

2. Меры по защите автоматизированных рабочих мест, с которых осуществляется работа в Аккаунтах

2.1. Требования к автоматизированным рабочим местам (далее – АРМ) при ведении Аккаунтов:

– на АРМ должно быть установлено лицензионное общесистемное и прикладное программное обеспечение (операционная система, интернет браузер и т.п.), а также выполнено обновление до актуальных версий, имеющих действующую техническую поддержку производителя;

– на АРМ должно быть установлено лицензионное антивирусное программное обеспечение (далее – ПО) с включением максимально возможного количества модулей защиты (межсетевой экран, система обнаружения вторжений, блокирование вредоносного ПО и других угроз, защита от сбора данных, обнаружение шпионского ПО и т.д.) и максимально возможного уровня защиты, с актуальными антивирусными базами;

– на АРМ необходимо настроить блокировку экрана при превышении определенного времени неиспользования АРМ (рекомендованное время простоя не более 5 минут).

2.2. Рекомендуется определить перечень рабочих мест, с которых осуществляется работа в социальных сетях. По возможности количество таких мест должно быть сведено к минимуму.

2.3. Не рекомендуется осуществлять работу в социальных сетях с мобильных устройств (мобильные телефоны, планшеты).

2.4. При необходимости осуществления доступа в социальные сети с мобильного устройства требуется исключить использование общедоступных Wi-Fi сетей, в связи с большой возможностью перехвата учетных данных владельцем Wi-Fi точки доступа.

3. Меры защиты при работе в Аккаунтах

3.1. Рекомендуемые настройки безопасности Аккаунтов[1]:

[1] Устанавливаются при наличии технической возможности в аккаунте социальной сети.

– обеспечить включение привязки номера телефона и дополнительного адреса электронной почты к Аккаунтам;

– обеспечить включение двухфакторной аутентификации – по логину, паролю и по СМС сообщению на телефон;

– использовать надежный пароль для каждого Аккаунта:

а) пароль должен содержать не менее восьми символов;

б) пароль должен содержать символы верхнего и нижнего регистров;

в) пароль должен содержать комбинации букв и цифр, по возможности – спецсимволы (!@#$%^&);

г) пароль не должен нести смысловой нагрузки, в качестве пароля не рекомендуется использовать часто употребляемые слова;

д) использовать уникальные пароли для различных Аккаунтов;

е) не использовать для записи паролей: стикеры, блокноты, а также иные способы, не обеспечивающие сохранение их в тайне;

ж) пароль рекомендуется периодически изменять (один раз в 3 месяца).

В случае подозрения на компрометацию пароля или увольнения/изменения ответственного лица за ведение Аккаунтов необходимо изменить пароль и данные для восстановления доступа к Аккаунтам;

– необходимо хранить данные о восстановлении доступа к Аккаунтам в актуальном состоянии и в надежном месте (например, в личном сейфе).

3.2. При авторизации в Аккаунтах необходимо проверять подлинность адреса страницы в сети "Интернет" и наличие актуального сертификата (рис. 1, рис. 2). При отсутствии сертификата вводить логин и пароль запрещается.

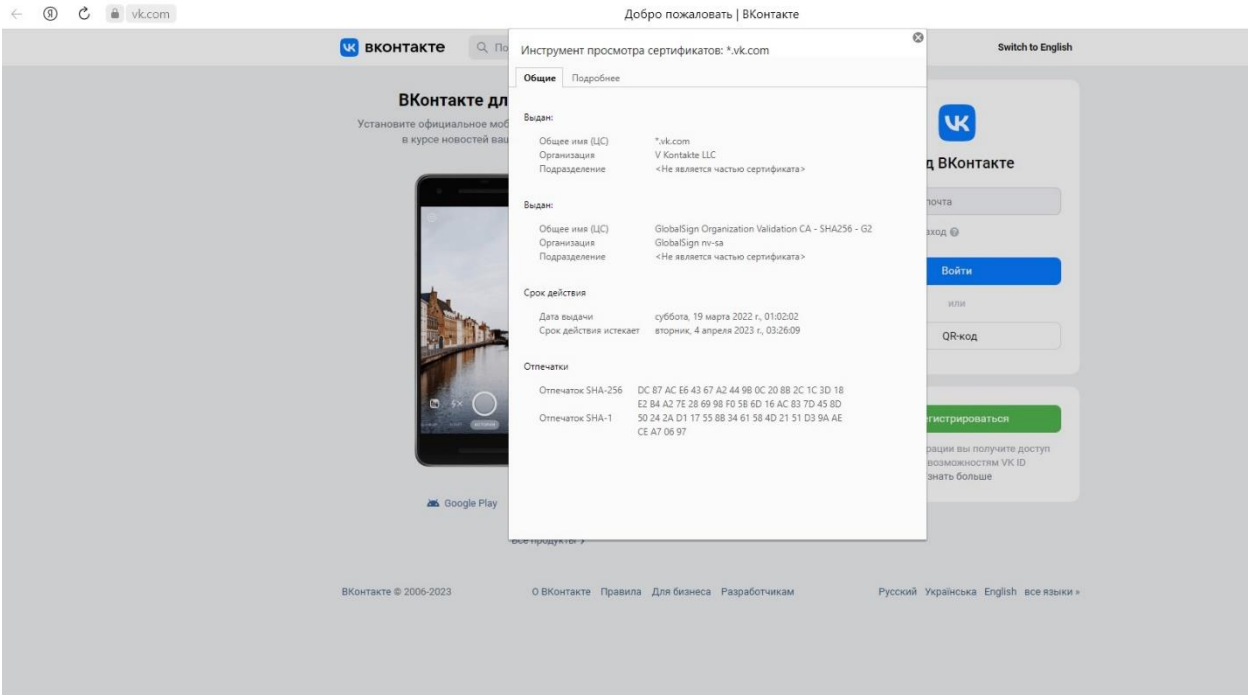

Рисунок 1 – сертификат на портале "ВКонтакте"

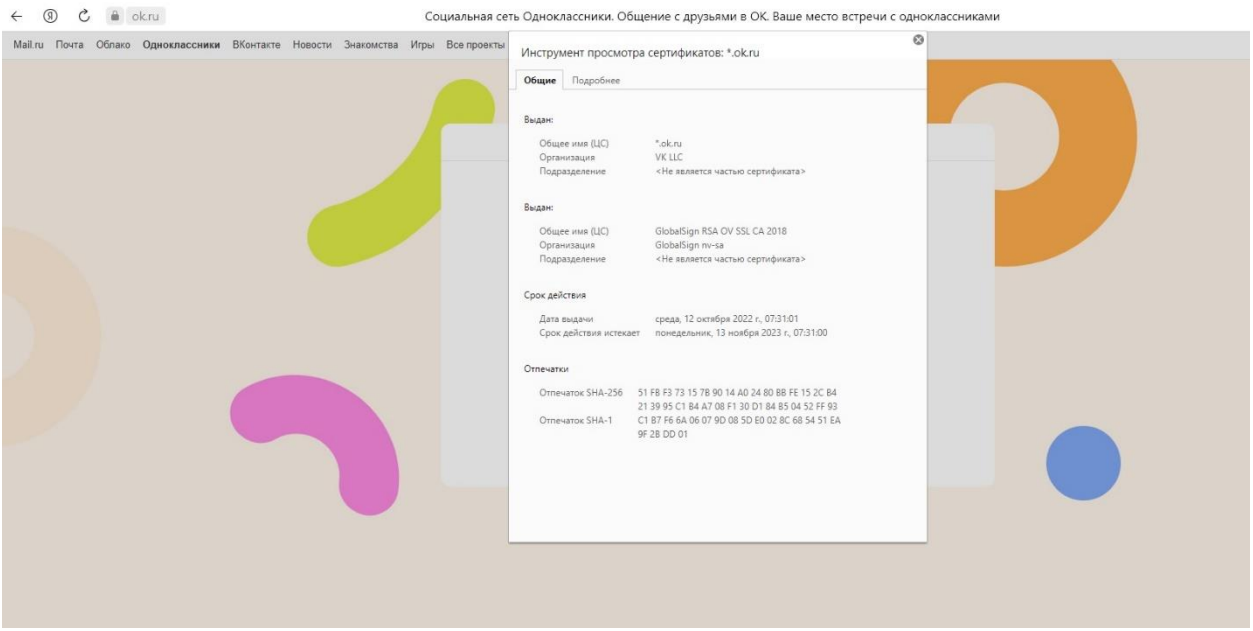

Рисунок 2 – сертификат на портале "Одноклассники"

3.3. По завершению работы в социальных сетях рекомендуется осуществлять выход из Аккаунтов.

3.4. При работе на АРМ в сети "Интернет" необходимо соблюдать общие правила, в том числе:

– не скачивать и не запускать подозрительные файлы;

– не переходить по подозрительным ссылкам, в том числе размещенным в комментариях;

– не посещать подозрительные ресурсы, сайты с ошибками или с отсутствующими сертификатами, вводить на данных сайтах логины и пароли.

3.5. При работе на АРМ с электронной почтой необходимо проверять полученные письма на "спам", а также на наличие вложений и ссылок.

При наличии вложений удостоверьтесь, действительно ли письмо предназначается Вам. В случае возникновения подозрений уточните у отправителя по иному каналу связи, не обозначенному в письме (например, телефон), о направлении в Ваш адрес письма с вложением. Вложение всегда размещается под полем "Кому" (рис. 3).

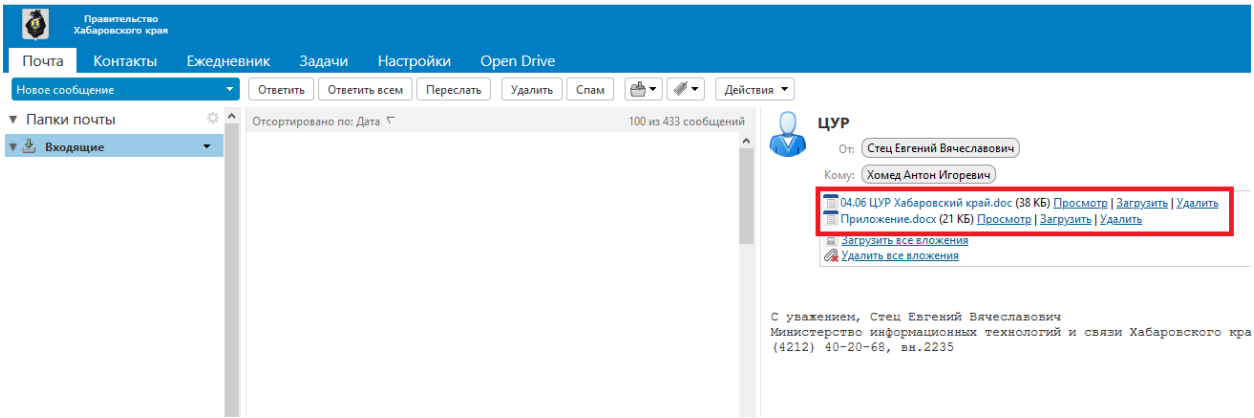

Рисунок 3 – вложение в почте

При наличии в письме ссылок, картинок, кнопок и т.д. запрещается нажимать на данные "активные" элементы, что может повлечь переход на

зараженные вирусом веб-ресурсы в сети "Интернет" или скачивание файлов, зараженных вирусами. При необходимости перехода на указанные в письме ресурсы рекомендуется адрес ресурса самостоятельно вводить в адресную строку браузера.

При получении писем о блокировке, подозрении на взлом, взломе Аккаунтов, необходимости изменения паролей или другой учетной информации запрещается переходить по ссылкам, указанным в письме.

Для проверки доступности Аккаунта необходимо самостоятельно ввести в адресную строку браузера адрес ресурса, о котором сообщено в письме и удостоверится в доступности Аккаунта. При необходимости сменить пароль.

3.6. Обращаем внимание, что службы технической поддержки официальных сайтов, порталов, сервисов никогда не запрашивают пароли пользователей.

_____