Приложение 3
УТВЕРЖДЕНО
Приказом Временной администрации по управлению банком
АО «Севастопольский Морской банк»
от 12.05.2020 г. № ВА/152

ПАМЯТКА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ КЛИЕНТОВ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Использование услуг дистанционного банковского обслуживания (далее – **ДБО**) сопряжено с риском получения несанкционированного доступа к конфиденциальной информации Клиента и осуществления переводов денежных средств со счетов неуполномоченными лицами.

Средства и методы защиты информации, применяемые Банком при предоставлении услуг ДБО, позволяют обеспечить необходимый уровень безопасности при условии выполнения Клиентом следующих рекомендаций:

1. Общие рекомендации при работе в системе ДБО

1.1 На рабочей станции, используемой для обеспечения работы системы ДБО, должно быть установлено и включено антивирусное программное обеспечение и персональный сетевой экран с постоянно обновляющимися в автоматическом режиме антивирусными базами.

1.2 Программное обеспечение, установленное на рабочей станции, используемой для обеспечения работы системы ДБО, должно быть либо лицензированным, либо получено из достоверного источника.

1.3 Должна быть отключена возможность автозапуска программ со всех подключаемых устройств хранения данных. Доступ к BIOS рабочей станции, используемой для обеспечения работы системы ДБО, должен быть закрыт паролем.

1.4 Не допускается хранение ключей электронной подписи непосредственно на жестких дисках рабочей станции, обеспечивающей работу системы ДБО, или иных встроенных в неё устройствах хранения данных. Для хранения ключей электронной подписи следует использовать съемные носители (диски, дискеты, съемные флеш-накопители, аппаратные средства электронной подписи).

1.5 Не допускается наличие на съемном носителе, используемом для хранения ключей электронной подписи, иной информации, кроме как ключевой, или использование его для любых иных целей. Любое устройство, используемое для хранения ключей электронной подписи, должно подключаться исключительно на время работы с системой ДБО, после чего должно отключаться в штатном порядке и перемещаться в место, предназначенное для его безопасного хранения (запирающийся металлический шкаф, сейф и т.д.).

1.6 Не допускается держать съемные носители ключевой информации постоянно подключенными к рабочей станции, их следует использовать только в случае необходимости.

1.7 Пользователи, имеющие полномочия работы с системой ДБО, не должны предоставлять исполнение своих обязанностей иным лицам, при любых обстоятельствах и для решения любых задач, кроме случаев, оформленных в официальном порядке.

1.8 Независимо от используемой операционной системы не рекомендуется работа пользователя на рабочей станции с правами администратора.

1.9 При увольнении сотрудников Клиента, имевших доступ к ключам электронной подписи и их носителям, обслуживающих систему ДБО или обеспечивающих информационно-техническую поддержку Клиента, необходимо незамедлительно заблокировать текущие и создать новые ключи электронной подписи, сменив также все пароли доступа. Также необходимо провести полную антивирусную проверку рабочей станции с установленной системой ДБО, а

также проверку на предмет запланированного исполнения каких-либо программ, наличия программ или компонентов программ удаленного доступа.

1.10 Вход в операционную систему рабочей станции с установленной системой ДБО должен обеспечиваться посредством ввода пароля. Количество неудачных попыток ввода пароля рекомендуется ограничить.

1.11 Пароли пользователей и администраторов должны иметь длину не менее 6 символов. В числе символов пароля рекомендуется использовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.). Срок действия паролей целесообразно ограничивать сроком в 2-3 месяца. Также желательно переименование учетных записей пользователей с административными правами.

1.12 Не допускается использование рабочей станции с установленной системой ДБО для каких-либо целей, отличных от целей, связанных с исполнением должностных обязанностей работника Клиента.

2. Рекомендации по безопасной работе в сети Интернет

2.1 Не следует отвечать и реагировать на сообщения, письма (e-mail, почтовые отправления и т.п.) или телефонные звонки, исходящие якобы от имени Банка, с просьбой выслать или сообщить иным образом ключ(и) электронной подписи, пароль(и) и другие конфиденциальные данные, установить программное обеспечение и т.д. Банк никогда не запрашивает у клиентов конфиденциальную информацию. Необходимое для работы системы ДБО программное обеспечение и иную информацию можно получить исключительно на официальном сайте Банка или непосредственно в Банке.

2.2 Не следует открывать письма или сообщения, полученные из неизвестных источников, устанавливать и запускать программы, прилагающиеся к письмам, и переходить по ссылкам из писем или сообщений.

2.3 Не следует вводить конфиденциальные данные, если окно для ввода отличается от стандартных окон (логотип другого банка, другие надписи, шрифт и тому подобное) или отображается не так, как всегда (нарушен порядок работы в системе). Необходимо внимательно следить за сообщениями, которые появляются на экране рабочей станции.

2.4 Рекомендуется исключить возможность просмотра ресурсов сети Интернет, если же это невозможно в силу причин производственного характера, то рекомендуется ввести ограничение на просмотр лишь тех ресурсов, которые необходимы при осуществлении рабочей деятельности.

2.5 Настройки безопасности программ, применяемых для просмотра ресурсов сети Интернет, должны обеспечивать максимальный уровень защиты, не препятствующий исполнению пользователем своих служебных обязанностей.

3. Действия при обнаружении случая несанкционированного доступа к счету

3.1 В случае если при включении рабочей станции, используемой для работы в системе ДБО, или в процессе работы системы ДБО будут обнаружены какие-то не имевшие ранее места события, такие, как нештатные информационные окна, сообщения об ошибках, сообщения о неверном ключе доступа или пароле, и т.п. – лицу, ответственному за работу с системой ДБО, необходимо зафиксировать суть события и незамедлительно уведомить о событии уполномоченных сотрудников Банка. Эти же действия необходимо выполнить и в случае появления признаков заражения вредоносными программами этой рабочей станции или вычислительной сети, к которой она подключена.

3.2 Ключи и пароли доступа к системе ДБО, равно как и пароли к рабочей станции, обеспечивающей функционирование системы ДБО, должны обязательно меняться в случае заражения данной рабочей станции вредоносными программами, только после процедуры проверки и удаления вредоносных программ.

3.3 При обнаружении электронного платежного документа, который заведомо не проводился на клиентской стороне уполномоченным лицом, необъяснимого изменения остатка средств на счете, или иных признаков, свидетельствующих о несанкционированном доступе к системе ДБО посторонних лиц, необходимо немедленно связаться с Банком, с целью принятия Банком своевременных мер, направленных на предотвращение негативных последствий.

3.4 После этого необходимо заблокировать действующие ключи электронной подписи и отключить рабочую станцию от внутренней компьютерной сети и сети Интернет.

СОГЛАСОВАНО:

Начальник Отдела информационной безопасности 05.02.2020 г. _____ / Е.И. Краснов

Начальник Управления информационных технологий 05.02.2020 г. _____ / Я.Г. Калуженко

Начальник Управления методологии 05.02.2020 г. _____ / Д.В. Шиян