СБЕРБАНК
Всегда рядом

ВНИМАНИЮ КЛИЕНТОВ!

Рекомендации по соблюдению мер информационной безопасности при работе с АРМ «Клиент» СПЭД

В настоящее время против клиентов систем ДБО коммерческих банков активно действуют хакерские группы, которые внедряют на персональных компьютерах (ПК), подключенных к сети Интернет, вредоносное программное обеспечение (ПО), позволяющее злоумышленникам осуществлять удаленный доступ к ПК клиентов и несанкционированную отправку фальшивых платежных документов. После этого мошенники стараются вывести ПК клиента из строя с целью скрытия факта списания средств от клиента и обеспечения возможности обналичивания похищенных средств.

Внедрение указанного зловредного ПО на ПК клиентов производится с использованием вирусных программ, массово распространяемых в сети Интернет через взломанные сайты, социальные сети и другие сетевые сервисы, электронную почту, свободно распространяемое ПО и пр. Через сайты российских и международных социальных сетей (odnoklassniki.ru, vkontakte.ru, facebook.com и т.д.) и через рекламно-баннерные сети распространяется наибольшее количество вредоносных программ. При этом новые модификации вирусов, сигнатуры которых еще не включены в антивирусные базы, успешно преодолевают антивирусное ПО.

При обнаружении на компьютере клиента ПО или адресов систем ДБО вирус связывается с управляющим сервером, размещаемым, как правило, за рубежом, и обеспечивает злоумышленникам полный контроль и удаленное управление зараженным ПК.

В этих условиях только жесткая политика в отношении свободного доступа в Интернет и постоянное соблюдение всего комплекса мер информационной безопасности, приведенных в Памятке, позволяет минимизировать риск мошеннических действий против клиентов, обслуживающихся через систему СПЭД.

1. Меры сетевой безопасности:

1.1. Для организаций, осуществляющих связь с банком с использованием коммутируемого доступа, подключение ПК с АРМ «Клиент» СПЭД к сети Интернет не допускается.

1.2. Настройками сетевого оборудования, корпоративных и персональных сетевых экранов выход в сеть Интернет ограничивается «белым списком» со всех ПК, на которых установлены АРМ «Клиент» СПЭД и осуществляется подготовка, подписание и отправка платежных документов. В «белый список» должны включаться исключительно доверенные сайты и хосты самой организации, банков, налоговой службы, других государственных органов, необходимых в

производственном процессе, сервера обновлений системного и антивирусного ПО. Доступ к иным информационным ресурсам и сервисам сети Интернет, включая электронную почту, социальные и пиринговые сети, конференции и чаты, телефонные сервисы и т.п. должен быть исключен.

1.3. Для ПК с АРМ «Клиент» СПЭД, с которых осуществляется отправка документов в банк, необходимо использовать встроенные средства сетевой фильтрации ПАК «ФПСУ-IP/Клиент».

В качестве защитной меры безопасности Банк применяет на устройствах ФПСУ-IP/Клиент принудительную глобальную настройку, блокирующую все новые попытки сетевых подключений к компьютеру Клиента во время установленного с Банком защищенного соединения. Данная политика действует только при соединении ПО ФПСУ-IP/Клиент с Банком и отключается при разрыве соединения. В связи с этим на ПАК ФПСУ-IP/Клиент должна быть настроена локальная политика фильтрации.

Наиболее простой конфигурацией локальных политик встроенного сетевого фильтра ПО ФПСУ-IP/Клиент является запрет всех подключений к ПК с АРМ «Клиент» СПЭД кроме соединений в локальной сети организации, например (показано на рис.1):

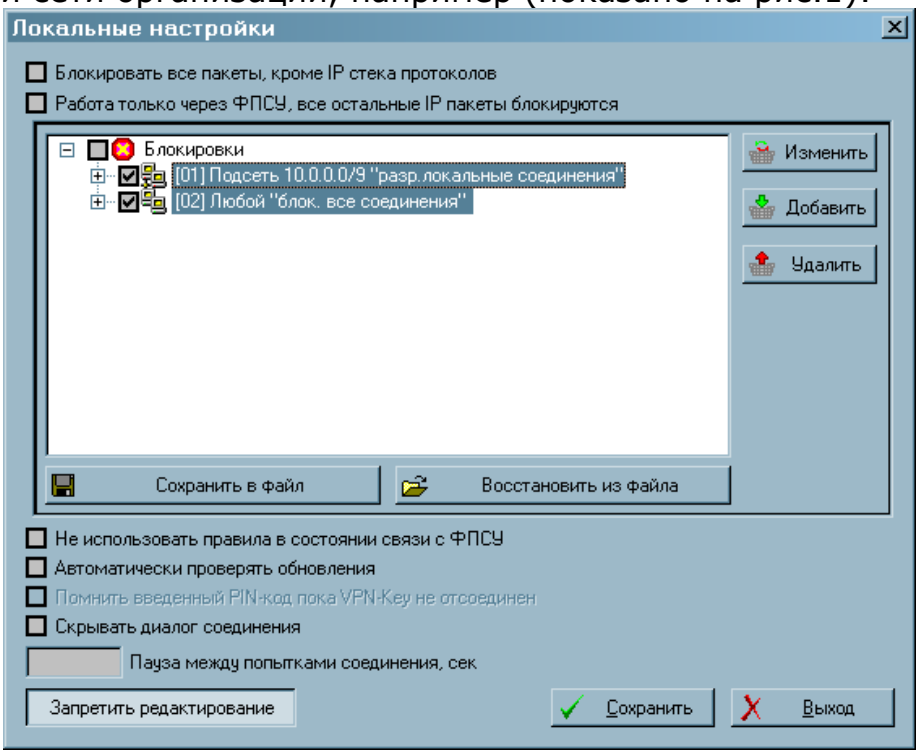

Рис.1.

Для защиты от угроз со стороны локальной сети рекомендуется конфигурацию локальной политики ПО «ФПСУ-IP/Клиент» усилить и настроить доступ только на необходимые в производственных целях ресурсы ЛВС, например, прописать адрес файлового сервера или ПК, на котором осуществляется подготовка платежных документов, сервер управления антивирусным ПО и пр. (см. рис.2).

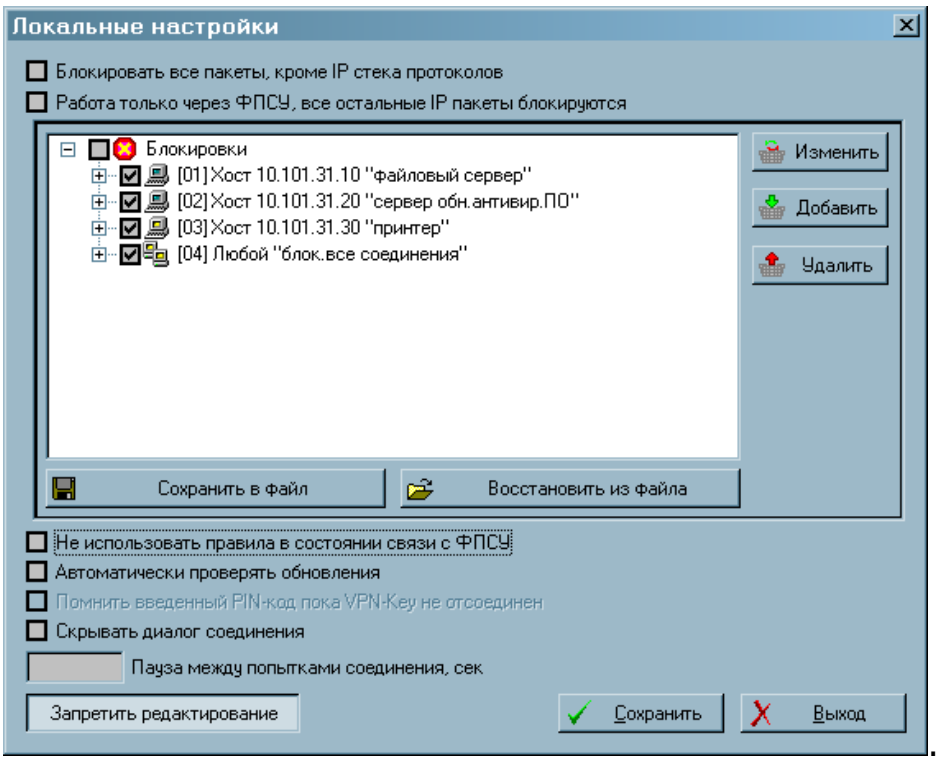

Рис.2.

При установке АРМ «Клиент» СПЭД на автономный ПК, не подключенный к ЛВС организации, а только к сети Интернет, в ПО «ФПСУ-IP/Клиент» может быть использована наиболее жесткая локальная сетевая политика, запрещающая все сетевые соединения кроме соединения с Банком по VPN (рис.3).

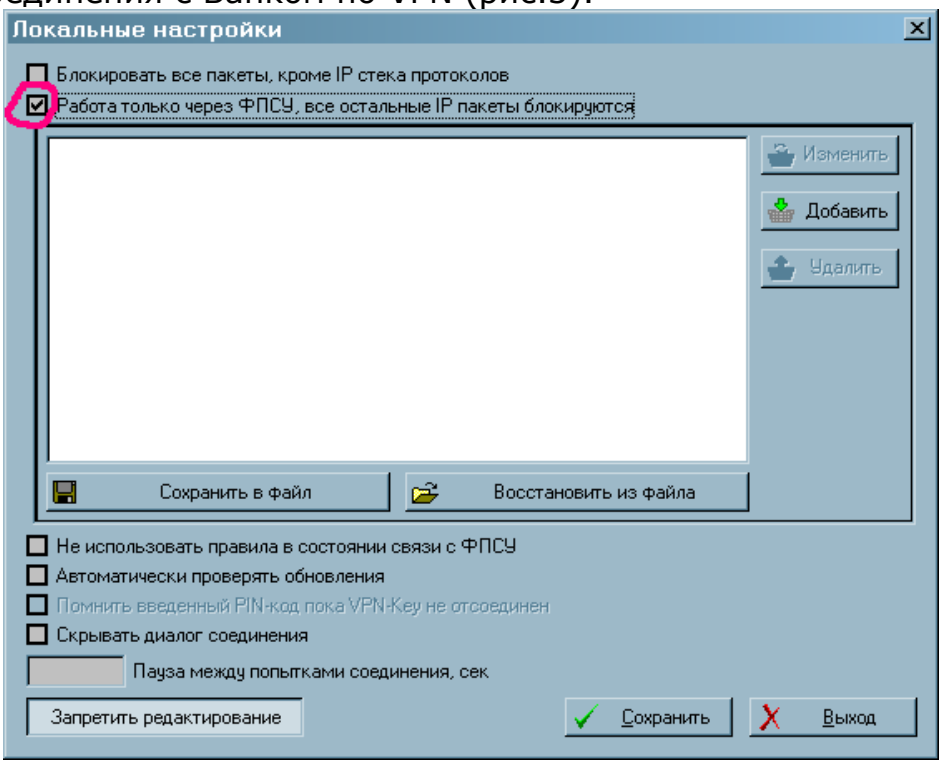

Рис.3

В этом случае риск реализации угроз из сети Интернет минимален.

2. Меры по защите от вредоносного ПО:

2.1. Перед установкой ПО АРМ «Клиент» СПЭД на ПК, проведением настроек безопасности в процессе его работы, необходимо проверить ПК на отсутствие вредоносного ПО, программ удаленного доступа к ресурсам ПК (TeamViewer, BeTwin, RAdmin и др.), программ работы с вирусоопасными ресурсами и сервисами сети Интернет, включая почтовые клиенты (см. раздел 1). При проведении таких проверок рекомендуется осуществлять загрузку ОС с внешнего эталонного загрузочного диска.
2.2. Должны быть установлены последние пакеты обновлений (Service Packs) и актуальные патчи безопасности ОС Windows, базы антивирусного ПО, обновление которых должно проводиться регулярно.
2.3. В ОС должна быть отключена функция AutoRun и настроен персональный сетевой экран ПО «ФПСУ-IP/Клиент» (см. раздел 1 памятки).
2.4. У пользователей ПК в ОС не должно быть административных прав и прав Power User («Опытный пользователь»).
2.5. Для исключения ошибочных и преднамеренных действий пользователя, приводящих к снижению защищенности системы и рискам финансовых потерь, необходимо средствами политик безопасности операционной системы или специализированными средствами защиты ПК от НСД обеспечить для пользователя функционально-замкнутую среду, позволяющую ему запускать и работать только с разрешенными программами без доступа к файловой системе и реестру ОС.
2.6. Необходимо исключить установку на ПК с АРМ «Клиент» СПЭД ПО, полученного из не заслуживающих доверия источников, а также нелицензионного и свободно-распространяемого ПО. Обращаем Ваше внимание, что подразделения ОАО «Сбербанк России» не рассылают обновления ПО АРМ «Клиент» СПЭД средствами почтовой связи или путем пересылки по электронной почте. Обновление версии АРМ «Клиент» СПЭД производится автоматически, встроенными средствами системы.
2.7. Не привлекать для администрирования и обслуживания АРМ «Клиент» СПЭД ИТ-персонал на условиях предоставления ему удаленного доступа.

3. Меры, направленные на защиту от копирования ключевой и парольной информации:

3.1. Настоятельно рекомендуется входить в АРМ «Клиент» СПЭД только для подготовки, отправки или получения информации в / из Банка. Нельзя оставлять АРМ «Клиент» СПЭД особенно с носители с ключевой информацией ЭЦП в рабочем состоянии без необходимости на продолжительное время. Например, не рекомендуется запускать АРМ «Клиент» СПЭД в начале рабочего времени, а выходить из него в конце рабочего времени. Вход и выход в АРМ должен происходить для осуществления конкретных действий сотрудника организации. После

чего носители с ключевой информацией ЭЦП сразу отключить и убрать в место хранения (сейф, и т.п.).
3.2. Необходимо выполнять незамедлительную блокировку и смену ключей ЭЦП в случаях их компрометации, а также по истечении срока действия ключей с периодичностью, установленной договорами и документацией.
3.3. Необходимо заменять ключи ЭЦП во всех случаях увольнения или смены руководителей юридического лица, подписывавших распоряжения (доверенности) о предоставлении сотрудникам организации полномочий подписания ЭЦП электронных документов.
3.4. При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения, а так же с использованием писем на «официальном» бланке лиц с просьбами сообщить или передать конфиденциальную информацию (ключи, пароли и пр.) ни при каких обстоятельствах не сообщать данную информацию.

4. Меры по контролю несанкционированных списаний:

4.1. Необходимо проводить контроль наличия платежных документов, находящихся в статусе «В почте», сразу после входа в АРМ «Клиент» СПЭД до первого выхода на связь с Банком, и контролировать количество и сумму отправленных документов по представлению Исходящие / Платежные поручения.
4.2. Следует регулярно контролировать состояние своих счетов и незамедлительно информировать обслуживающее подразделение Банка обо всех подозрительных или несанкционированных операциях.
4.3. В случае неожиданного выхода из строя компьютера, либо пропадания на нём программного обеспечения АРМ «Клиент» СПЭД, необходимо прекратить на ПК работу, отключив его от всех видов сетей, включая локальную корпоративную сеть, и модемов, срочно запросить в Банке выписку по счету, используя АС «Voice Informator» (если данная услуга подключена), либо непосредственно в Банке. При обнаружении несанкционированных платежных операций написать заявление в Банк, а также обратиться с соответствующим заявлением в правоохранительные органы. Работоспособность поврежденного ПК не восстанавливать до проведения технической экспертизы. Переустановку АРМ «Клиент» СПЭД проводить на новом ПК. После переустановки АРМ «Клиент» СПЭД произвести немедленную смену всех своих ключей ЭЦП.
4.4. Появление на экране ПК во время отсутствия соединения с банком сообщений, провоцирующих на установление такого соединения (например, сообщения о необходимости подключения токена ФПСУ-IP/Клиент к USB-порту и выполнении соединения с сервером), свидетельствует о наличии на ПК вредоносного ПО.
Описание подобного вредоносного ПО можно получить в сети Интернет на сайте ООО «Амикон» по ссылке www.amicon.ru/virus.php.
В данной ситуации установление соединения с банком может привести к отправке фальшивого документа. При появлении подобного

сообщения необходимо провести контроль платежных документов, находящихся в статусе «в почте». Далее в любом случае действовать согласно п.4.3 настоящей памятки. Помните, что реальные сообщения от Банка могут быть получены только в режиме установленного соединения.

5. Меры по поддержанию уровня информационной безопасности

Для обеспечения высокого уровня информационной безопасности при эксплуатации АРМ «Клиент» СПЭД в организации должен быть назначен ответственный, который осуществляет:

5.1. Постоянный контроль соблюдения мер информационной безопасности, предусмотренных настоящей памяткой, документацией на систему и средства защиты,

5.2. Выявление, устранение и информирование руководства организации обо всех выявленных нарушениях,

5.3. Контроль устранения выявленных нарушений,

5.3. Документирование результатов проведенных работ и проверок,

5.4. Организацию и проведение мероприятий по усилению безопасности в соответствии с информационными сообщениями, которые направляются Банком непосредственно по системе, прилагаются к Сообщениям из банка, официальными письмами, а также публикуются на сайте Банка.