Приложение № 14
к Регламенту работы в системе ИНТЕРНЕТ-БАНК»
в ООО «Банк РСИ»

Рекомендации о мерах по обеспечению информационной безопасности

1. Организационные меры

1.1. Логин пароль и СКЗИ JaCarta ГОСТ (*системы ИНТЕРНЕТ-БАНК»)* должны храниться в сейфе, доступ к которому должен быть строго ограничен: лица, обладающие правом подписи на документах, бухгалтер, работающий с системой «Клиент-Банк»» по доверенности – далее «уполномоченные лица».

Хорошей практикой является хранение вышеуказанных носителей в сейфе в **опечатанном контейнере**. Целостность печати (пломбы) должна ежедневно, в начале рабочего дня, контролироваться руководителем организации или уполномоченным лицом. После завершения работы ключевой носитель помещается в контейнер и заново опечатывается (пломбируется) уполномоченным лицом.

Не держите ключевые носители постоянно вставленными в компьютер, используйте их только в случае необходимости заверки платежных документов.

1.2. Категорически **запрещается использовать компьютер**, на котором развернута программа (*системы ИНТЕРНЕТ-БАНК»)* (далее - компьютер), для просмотра посторонних (не относящихся к *системе «ИНТЕРНЕТ-БАНК»* Интернет сайтов, работы с электронной почтой (особенно через общедоступные почтовые Web-сервера: Mail.ru и т.д.), запрещается устанавливать и использовать программы мгновенных почтовых сообщений (ICQ, QIP и т.д.), запрещается пользоваться Skype, устанавливать игры и любые программы с пиратских дисков, просматривать видеофильмы, слушать музыку, загружать и устанавливать любые программы из Интернет, открывать и редактировать непроверенные антивирусом DOC, XLS, PDF файлы.

Пожалуйста, не пожалейте средств на выделение отдельного компьютера для работы только с *системой «ИНТЕРНЕТ-БАНК»* **!**

1.3. В случае **временного перерыва в работе** с компьютером (совещание, обед, «перекуры» и т.д.) необходимо завершить работу с *системой «ИНТЕРНЕТ-БАНК»*, убрать в сейф СКЗИ JaCarta ГОСТ, выключить компьютер или, как минимум, заблокировать его клавиатуру и экран путем нажатия клавиш Ctrl-Alt-Del.

1.4. **Запрещается записывать пароли** на бумажных листках (или в текстовых файлах на компьютере), оставлять их в легкодоступных местах (на рабочем столе), передавать неуполномоченным лицам. Если есть необходимость – храните все пароли, записанными на одном листе, в сейфе, в опечатанном контейнере вместе с ключевым носителем.

1.5. **Компрометация системы** *«ИНТЕРНЕТ-БАНК»*, это:

а). Любые кадровые перестановки лиц, имевших доступ к компьютеру и ключам (в т.ч. увольнение системного администратора).

б). Любые Ваши подозрения в несанкционированном доступе (локально или по сети) неуполномоченных лиц к компьютеру, ключам, программе *«ИНТЕРНЕТ-БАНК»*, паролям.

в). Обнаружение вируса на компьютере.

г). Работа на компьютере с Интернет без включенной защиты (антивирус с активным монитором + файрвол (класс: не выше 4) (персональным экраном), просмотр Интернет – сайтов, не относящихся к *«ИНТЕРНЕТ-БАНК»*, установка любых программ с нелицензионных дисков или по сети.

В случае возникновения компрометации Вам необходимо срочно связаться со специалистами Банка любым доступным способом, сообщить название Вашей организации, номер договора (Ваш идентификатор системы *«ИНТЕРНЕТ-БАНК»*, для службы технической поддержки) и

детально описать что произошло. Это позволит нам оперативно заблокировать доступ к Вашему счету через *«ИНТЕРНЕТ-БАНК»*.

2. Технические меры

2.1. **Физический доступ** к компьютеру должен быть ограничен и предоставлен **только** уполномоченным лицам. Рекомендуется использовать следующие методы защиты физического доступа к компьютеру:

а). Установка пароля **BIOS** на включение компьютера и на вход в настройки BIOS.

б). Установка пароля на включение операционной системы Windows с помощью команды **syskey.**

в). Вход в Windows должен выполняться путем ввода имени пользователя и его пароля. Пароли учетных записей пользователей и администратора должны быть сложными, не должно быть учетных записей с пустыми паролями.

г). Пользователь «Гость» **(«Guest»)** обязательно должен быть заблокирован.

д). Системный блок компьютера должен быть **опечатан пломбой (или голографической наклейкой, стикером)**, целостность пломбы (наклейки, стикера) должна регулярно контролироваться уполномоченным лицом.

е). Как дополнительное средство защиты можно использовать **аппаратный модуль доверенной загрузки** (программное средство, обеспечивающее защиту от несанкционированного доступа и контроль целостности информации до загрузки операционной системы).

ж). Как дополнительное средство защиты можно использовать **разрешения файловой системы NTFS**, а именно: предоставить полный доступ к папке (и всем вложенным в нее папкам и файлам), в которой находится программа *«ИНТЕРНЕТ-БАНК»*, пользователю, работающему с «Клиент-Банк», и указать **явный запрет** на доступ к этой папке для всех остальных пользователей.

з). В операционной системе должен быть включен системный аудит, регистрирующий возникающие ошибки, вход пользователей и запуск программ, необходимо периодически просматривать журнал и реагировать на ошибки.

и). Контролировать состояние своего счета в Банке (путем просмотра выписки).

к). Обращать внимание на дату и время последних входов в систему «Клиент-Банк».

2.2. На компьютере должно быть установлено или встроенное в операционную систему, и регулярно обновляться лицензионное **антивирусное программное обеспечение и его базы данных**. Монитор антивируса должен быть постоянно включен с момента загрузки компьютера. Должно быть настроено регулярное **автоматическое сканирование** оперативной памяти и жестких дисков компьютера на наличие вирусов.

2.3. На компьютере должен быть **включен файрвол (встроенный в Windows или установлен и включен персональный экран стороннего производителя)** и заблокирован несанкционированный **входящий** трафик по всем TCP и UDP портам для всех адресов, как Интернет (настроить персональный экран по принципу: запрещено все, что не разрешено), так и локальной сети, запретить работу по протоколам ftp, smtp. На компьютере должна быть **остановлена и запрещена для запуска служба Server, остановлена и запрещена служба удаленного управления реестром Windows.** Это приведет к невозможности доступа к компьютеру по сети, что повлечет, однако, ряд ограничений: на этом компьютере нельзя будет создавать общие сетевые папки и предоставлять доступ к его локальному принтеру по сети для других компьютеров Вашей организации.

Тем не менее, **применение этой меры является необходимым**, так как оно обеспечивает (при условии соблюдения п. 1.2, 2.2.) сетевую информационную безопасность персонального компьютера с установленной системой *«ИНТЕРНЕТ-БАНК»*.

При наличии в Вашей организации грамотного системного администратора возможна более тонкая настройка файрвола – открытие определенных портов и адресов для правильного взаимодействия компьютера, например, с контроллерами домена, запрет на установку и исполнение любых несанкционированных программ (отслеживание вирусных атак на компьютер) и т.д.

Если в Вашей организации уже есть развернутая программная или аппаратная система сетевого экранирования, защищающая периметр сети, то включение собственного файрвола на

компьютере (при условии правильной его настройки и регулярном обновлении), все равно, является обязательным требованием – это Ваш последний рубеж обороны.

2.4. Компьютер должен регулярно обслуживаться грамотным системным администратором и только в присутствии уполномоченного лица. Администратор должен подробно объяснять Вам, какие действия и с какой целью он выполняет в настоящее время. Необходимо выполнять следующие **регулярные работы**: проверка успешности функционирования антивируса и файрвола, полное сканирование компьютера антивирусом, обновление антивируса и файрвола, установка необходимых обновлений операционной системы Windows (установка патчей, критичных обновлений системы безопасности). Во время проведения этих работ ключевой носитель должен находиться в сейфе!

2.5. Не использовать права администратора при отсутствии необходимости. В повседневной практике (особенно при работе с *«ИНТЕРНЕТ-БАНК* входить в систему как пользователь, не имеющий прав администратора.

2.6. Обязательно **смените пароль** на вход в систему *«ИНТЕРНЕТ-БАНК* в соответствии с инструкцией, выдаваемой вместе с СКЗИ JaCarta ГОСТ.

Внимание! При смене, увольнении лица, имеющего даже потенциально, доступ к ключевому носителю (например, системного администратора), необходимо незамедлительно:

- **сменить пароль доступа в систему**
- **заблокировать скомпрометированный ключевой носитель (установленным порядком) и получить новый в Банке.**

НАСТОЯТЕЛЬНО ПРОСИМ ВАС НЕЗАМЕДЛИТЕЛЬНО ОБРАЩАТЬСЯ В БАНК ПРИ ВОЗНИКНОВЕНИИ СЛЕДУЮЩИХ СИТУАЦИЙ:

- у Вас не работает система *«ИНТЕРНЕТ-БАНК* по неизвестным («необычным») причинам (например, Вы не можете войти в систему, т.к. возникает «ошибка авторизации», говорящая о неправильно набранном пароле, хотя пароль Вы набираете на клавиатуре верно или вход в систему заблокирован, невозможно связаться с банковским сервером *«ИНТЕРНЕТ-БАНК»*, необычная работа известных программ и т.п.).
- Обнаружены (или есть подозрения на несанкционированный доступ к Вашей информации) факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время и т.п.).
- В выписке обнаружены несанкционированные Вами расходные операции.

Обращаем Ваше внимание, что своевременное обращение в Банк позволит принять оперативные меры по предотвращению мошенничества и сохранить Ваши средства.

Клиент

_____

_____(_____)

М.П.