Приложение № 4
к Договору дистанционного банковского обслуживания с
использованием Системы «iBank»
в АО «Тольяттихимбанк»

Требования к обеспечению информационной безопасности при использовании Системы «iBank»

1. **Вниманию Клиента.**

1.1. Согласно статистике, наиболее **часто попытки хищения** денежных средств **осуществляются**:

1.1.1. **Работниками, в том числе уволенными, имеющими или имевшими доступ к носителям ключей электронной подписи, а также доступ к АРМ.**

1.1.2. **IT-специалистами (штатными и внештатными), оказывающими (или оказывавшими ранее, в т.ч. однократно) различные IT-услуги по поддержке, подключению к сети Интернет, установке, обновлению и поддержке различных программ (бухгалтерских, правовых, информационных и др.) на АРМ.**

1.1.3. **Мошенниками, с использованием сети Интернет, путём заражения АРМ ВК, использования уязвимостей в безопасности АРМ и корпоративной сети с последующим хищением через сеть Интернет Закрытого (секретного) ключа ЭП, пароля ключа ЭП.**

1.2. Во всех перечисленных в пп. 1.1.1 – 1.1.3 случаях, злоумышленники, завладев З**акрытым (секретным) ключом ЭП** и **паролем ключа ЭП** или путем перехвата управления АРМ Клиента, направляют от имени Клиента в Банк электронные расчетные документы для перевода денежных средств со счетов Клиента различным физическим и юридическим лицам.

1.3. Банк не осуществляет рассылку электронных писем с просьбой прислать Закрытый (секретный) ключ ЭП и/или пароль к ключу ЭП и никогда не запрашивает у Клиентов эту информацию.

1.3.1. **Рассылка программ (или ссылок на них) по электронной почте для установки на АРМ Клиента может осуществляться только службой технической поддержки Клиентов Системы «iBank» Банка и только по предварительной договоренности с работниками Клиентов.**

1.3.2. **Не следует выполнять указания, в случае получения Клиентом подобного «сомнительного» письма от имени Банка, содержащего программу для установки или запрос на предоставление Закрытых (секретных) ключей ЭП Клиента, паролей к ключу ЭП, используемых в Системе «iBank». О произошедшем необходимо незамедлительно сообщить в службу технической поддержки Клиентов Системы «iBank» Банка.**

2. **Меры по обеспечению безопасности носителей с Закрытыми (секретными) ключами ЭП:**

2.1. **Для хранения Закрытых (секретных) ключей ЭП разрешается использовать только съемные носители (дискеты, компакт-диски (CD/DVD), Flash-накопители (флэшки), специальные устройства для хранения ключей электронной подписи).** Использование специальных устройств для хранения ключей электронной подписи **является наиболее безопасным.**

2.2. Хранить пару ключей ЭП каждого из Уполномоченных лиц Клиента на отдельном НЭК.

2.3. **Хранить НЭК в условиях, исключающих доступ к ним третьих лиц.** Для хранения НЭК должны использоваться индивидуальные надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

2.4. Использовать механическую блокировку функции записи на НЭК при её наличии.

2.5. **Извлекать НЭК из АРМ (отключать от АРМ) каждый раз после завершения их использования.** НЭК должны находиться в АРМ (подключаться к АРМ) только в момент подписания документов, даже если работа в Системе **«iBank»** продолжается, НЭК должны быть извлечены из АРМ (**отключены от АРМ**) сразу после окончания подписания документов.

2.6. **По завершении использования Системы «iBank» извлекать НЭК из АРМ (отключать от АРМ) и помещать их при этом для хранения в соответствии с условиями п. 2.3.**

2.7. **Не передавать Закрытые (секретные) ключи ЭП и НЭК кому-либо**, в том числе IT-специалистам, для проверки работы Системы «iBank», настроек взаимодействия с Банком и т.п. При необходимости таких проверок владелец Закрытого (**секретного) ключа ЭП** обязан подключать НЭК к АРМ лично.

2.8. **Запрещается:**

2.8.1. **Хранить Закрытые (секретные) ключи ЭП на жёстких или сетевых дисках АРМ**.

2.8.2. **Оставлять (даже на минимальное время) НЭК установленными в АРМ (подключенными к АРМ), если они не используются.**

2.8.3. **Хранить НЭК в свободном доступе (например, на столе) в тот момент, когда они не находятся в зоне «прямой видимости». В случае необходимости отлучиться от рабочего места следует поместить НЭК в защищённое место в соответствии с условиями п. 2.3.**

2.8.4. **Снимать несанкционированные копии с НЭК**.

2.8.5. **Передавать НЭК лицам, не допущенным к работе с НЭК**.

2.8.6. **Подключать НЭК к компьютерам не являющимися АРМ**.

2.8.7. **Выводить Закрытые (секретные) ключи ЭП на дисплей (монитор) компьютера или принтер**.

2.8.8. **Использовать НЭК для выполнения каких-либо иных функций, не связанных с работой в Системе «iBank»**.

2.8.9. **Хранить на НЭК какую-либо иную информацию кроме Закрытых (секретных) ключей ЭП**.

2.9. Определить и утвердить порядок учета, хранения и использования НЭК, который должен полностью исключать возможность несанкционированного доступа к НЭК.

2.10. Рекомендуется выполнить комплекс организационных мероприятий по обеспечению информационной безопасности в соответствии с технической документацией на используемое средство криптографической защиты информации и следующими нормативными документами:

2.10.1. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

2.10.2. Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

2.11. Исключить доступ посторонних лиц в помещения с клиентским АРМ.

3. **Обеспечить безопасность пароля к Закрытому (секретному) ключу ЭП Клиента используемому в Системе «iBank»:**

3.1. **Не назначать пароль, используемый в Системе «iBank», в любых других системах и сервисах.**

3.2. **Не сообщать пароль, используемый в Системе «iBank», кому-либо**, в том числе IT-специалистам для проверки работы системы, настроек взаимодействия с Банком и др. При необходимости таких проверок владелец Закрытого (секретного) ключа ЭП обязан лично вводить пароль к ключу ЭП в Систему «iBank».

3.2.1. Требования к паролю:

3.2.1.1. Длина пароля должна быть не менее восьми символов, состоящих из комбинации различных групп символов: букв верхнего и нижнего регистров латинского алфавита, цифр, специальных символов, знаков препинания и пунктуации, арифметических операций (если их использование в пароле явно незапрещено настройками АРМ).

3.2.1.2. Необходимо выбирать трудно подбираемые пароли.

3.2.1.3. При выборе паролей не должна использоваться какая-либо «система»: новый пароль не должен быть прогнозируемым на основе знаний о предыдущих паролях, датах их смены и т.д.

3.2.1.4. При выборе пароля запрещается:

3.2.1.4.1. Использовать пустые пароли.

3.2.1.4.2. Повторно использовать старые пароли. Новый пароль не должен совпадать ни с одним из предыдущих паролей. Новый пароль должен отличаться от предыдущего не менее чем в четырех символах.

3.2.1.4.3. Использовать в качестве пароля последовательность символов, состоящих из одних цифр. Например, «12349876», «03826495».

3.2.1.4.4. Использовать в качестве пароля идущие подряд (расположенные рядом) в раскладке клавиатуры символы. Например, «QWERTYUI», «qazxswEDC», «qazwsxedc».

3.2.1.4.5. Использовать в качестве пароля буквы, расположенные в прямом и в обратном алфавитном порядке, в том числе набранные на регистре другого языка. Например: «CDEFGHIJ» (идущие подряд буквы латинского алфавита), «zyxwVUTS» (буквы латинского алфавита в обратном порядке), «f,dult`;», (абвгдеёж – идущие подряд буквы русского алфавита, набранные на латинской раскладке клавиатуры).

3.2.1.4.6. Использовать в качестве пароля осмысленные слова (любого языка), сленговые выражения или общеупотребительные сокращения, имена собственные (названия, имена и фамилии), в том числе набранные на регистре другого языка или преобразованные транслитерацией. Например, «grapefruit» (грейпфрут (англ.)), «Churchill» (Черчилль (англ.)), «Zelenograd» (Зеленоград), «admin» (сленговое выражение, сокращенное от «administrator»), «cbcntvf» (система), «svetofor» (светофор).

3.2.1.4.7. Включать в пароль последовательности из четырех и более повторяющихся символов. Например, «qqqqqqqq», «ad111111» или «ZZZZaaaa».

3.2.1.4.8. Включать в пароль ассоциируемую с пользователем или АРМ информацию, которую легко узнать: Ф.И.О. сотрудника или его ближайших родственников, марку автомобиля, кличку домашнего животного, название АРМ в локальной сети, название сервера и т.д., например, «dmitry666» (если имя сотрудника – Дмитрий), «THBPass» (если пароль – к учетной записи для доступа в Систему «iBank»).

4. **Для АРМ, необходимо:**

4.1. **Применять для работы лицензионное программное обеспечение.**

4.2. **Использовать операционную систему, поддерживаемую производителем.**

4.3. **Рекомендуется использовать только последние версии браузера (программного обеспечения для просмотра веб-сайтов). Регулярно (не реже чем ежедневно) в автоматическом режиме производить обновление браузера.**

4.4. **Применять лицензионное средство защиты от ВК или защитное ПО.**

4.4.1. **Применять последние версии лицензионного средства защиты от ВК или защитного ПО.**

4.4.2. **Обеспечивать** регулярное обновление в автоматическом режиме баз данных ВК по мере их размещения (обновления) разработчиками средств защиты от ВК, но не реже чем ежедневно.

4.4.3. **О**беспечивать регулярный в автоматическом режиме ежедневный полный Контроль АРМ на наличие ВК.

4.4.4. Рекомендуется использовать средства защиты от ВК или защитное ПО, сертифицированные ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

4.5. **Обеспечить регулярную (не реже чем ежедневно) в автоматическом режиме загрузку и установку обновлений безопасности операционной системы**.

4.6. **Исключить загрузку и установку нелицензионного программного обеспечения. В особенности ПО, загруженного с неизвестных сайтов сети Интернет.**

4.7. **Осуществлять проверку на наличие ВК посредством средств защиты от ВК любых файлов и программ**, загружаемых из сети Интернет, полученных по электронной почте или на внешних носителях (дискеты, Flash-накопители (флэшки), CD/DVD и т.п.).

4.8. Рекомендуется включить автоматическое обновление и использовать последнюю версию виртуальной Java-машины.

4.9. **Исключить доступ к АРМ персонала, не имеющего отношения к работе с Системой «iBank».**

4.10. **Не допускать работу пользователей с Системой «iBank» под учётной записью операционной системы, имеющей права администратора.** Использовать учётную запись с ограниченными правами.

4.11. **Ограничить** локальными (или доменными) политиками на АРМ **список пользователей, имеющих право входа в операционную систему**.

4.12. **Все учетные записи пользователей АРМ должны быть защищены паролем**.

4.12.1. Следует осуществлять периодическую смену паролей (не реже 1 раза в месяц).

4.12.2. Ограничить количество неудачных попыток входа в систему. Рекомендуется блокировать вход после трех неудачных попыток.

4.12.3. Устанавливать пароли в соответствии с требованиями, установленными п. 3.2.1.

4.13. **Блокировать сетевой доступ к АРМ (в том числе запретить Дистанционное управление рабочим столом, Удаленный помощник) с других рабочих станций локальной сети и из внешних сетей, включая сеть Интернет.**

4.14. **Запретить использование любых средств удалённого (дистанционного) доступа**, которые обычно используется IT-специалистами для удалённой (дистанционной) поддержки.

4.15. **Полностью запретить все** (входящие и исходящие) **соединения с сетью Интернет, разрешив доступ только к IP-адресам сайтов Системы «iBank» Банка**.

4.16. Разрешить сетевое взаимодействие АРМ только с необходимым доверенным перечнем IP-адресов в локальной сети Клиента.

4.17. Для выполнения требований пунктов 4.13 – 4.15 рекомендуется применение лицензионного персонального межсетевого экрана (программного и/или аппаратного).

4.18. При наличии технической возможности подключения рабочей станции к сети Интернет со статического IP-адреса, подать заявку в Банк для подключения функции разрешения доступа Клиента только с фиксированного статического IP-адреса и использовать при работе в Системе «iBank» режим IP-фильтрации.

4.19. На АРМ должна быть установлена только одна операционная система.

4.20. Запретить использовать АРМ в публичных (проводных/беспроводных) сетях, предоставляющих доступ к сети Интернет, для исключения значительного повышения риска компрометации имени пользователя (логина) и пароля, используемых в Системе «iBank», секретных ключей ЭП Клиента.

4.21. Запретить устанавливать на АРМ средства разработки ПО и отладчики ПО.

4.22. Принять меры, препятствующие несанкционированному вскрытию системного блока АРМ.

4.23. Ограничить минимально необходимыми правами доступ на запись к файловым ресурсам АРМ.

4.24. Запретить пользователям АРМ запуск всех приложений, кроме приложений, необходимых для работы Системы «iBank».

4.25. Запретить подключать к АРМ внешние устройства, в том числе носители информации, не обусловленные производственной необходимостью.

4.26. Запрещается оставлять без контроля АРМ. При кратковременном отсутствии следует блокировать рабочее место средствами операционной системы.

4.27. Разрешить для АРМ загрузку только с носителя, на котором установлена операционная система. Отключить загрузку с других носителей (с гибкого диска, привода оптических дисков, загрузку по сети, загрузку со съёмных носителей и т.д.).

4.28. Отключить учетную запись для гостевого входа (Гость, Guest).

4.29. Запретить режим автоматического входа пользователя без ввода пароля в операционную систему при ее загрузке.

4.30. Запретить режим отображения окна всех зарегистрированных на АРМ пользователей и быстрое переключение пользователей.

4.31. Использовать штатные возможности операционной системы для защиты от ВК и несанкционированного доступа. В зависимости от используемой операционной системы, задействовать следующие встроенные механизмы защиты (при наличии):

4.31.1. Контроль учетных записей – механизм, упрощающий использование учетных записей, не обладающих административными привилегиями;

4.31.2. Брандмауэр – встроенный межсетевой экран;

4.31.3. Использование технологии AppLocker;

4.31.4. Защитник Windows – служба защиты от шпионского ПО;

4.31.5. Средство удаления вредоносных программ.

5. Использовать следующие меры обеспечения безопасности при работе с электронной почтой:

5.1. Запретить открывать письма и прикрепленные к ним файлы, полученные от неизвестных отправителей, переходить по содержащимся в таких письмах ссылкам.

5.2. **Д**ля сообщений электронной почты, используя **средства защиты от ВК или защитное ПО, о**существлять исключение из информационного потока сообщений, которые имеют признаки наличия ВК, или приостановление их обработки (помещение таких сообщений в карантин) с выдачей соответствующего уведомления.

6. **Рекомендуется:**

6.1. Организовать АРМ, предназначенное исключительно для работы с Системой «iBank» Банка.

6.2. **Осуществлять доступ к работе в Системе «iBank» уполномоченных лиц Клиента с разных АРМ.**

6.3. Подготовить, утвердить и проводить регулярное тестирование процедур реагирования на инциденты информационной безопасности при работе **в Системе «iBank»**.

7. **Принимать повышенные меры по обеспечению отсутствия ВК (как минимум, проверять работоспособность средств защиты от ВК и актуальность баз данных ВК, а также осуществлять полный Контроль АРМ на наличие ВК) в следующих случаях:**

7.1. **При увольнении штатного IT-специалиста (системного администратора)**, осуществлявшего обслуживание АРМ.

7.2. **После любых действий внештатных IT-специалистов** или любых других сотрудников, выполнявших любые операции на АРМ (например, решение каких-либо проблем, подключение к сети Интернет, установка, обновление и поддержка различных бухгалтерских, правовых, информационных и др. программ и т.п.).

8. **План действий в случае обнаружении факта несанкционированного Клиентом списания со счета(-ов) денежных средств**.

8.1. **При обнаружении факта несанкционированного Клиентом списания со счета(-ов) денежных средств, Клиент обязан немедленно:**

8.1.1. **не выключать АРМ(-ы), с которого(-ых) выполняется работа в Системе «iBank»;**

8.1.2. **физически отключить АРМ(-ы) от сети Интернет (отключить соединительный провод к устройству, посредством которого осуществляется доступ в сеть Интернет, или в случае если доступ осуществляется посредством оборудования, расположенного в локальной сети, от локальной сети);**

8.1.3. **сообщить о произошедшем в Банк;**

8.1.4. **сообщить о произошедшем в правоохранительные органы.**

9. **Требования по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет**.

9.1. Для входа в Систему «iBank» следует набрать в адресной строке браузера: https://ibank.thbank.ru.

9.2. Прежде чем ввести имя пользователя (логин) и пароль, используемые в Системе «iBank», еще раз внимательно проверить в адресной строке браузера адрес сайта – https://ibank.thbank.ru.

10. **Рекомендации по защите АРМ от несанкционированного доступа**.

10.1. Для защиты АРМ от несанкционированного доступа на АРМ установить программно-аппаратный комплекс защиты от несанкционированного доступа.

10.2. Сформировать с помощью комплекса защиты от несанкционированного доступа функционально замкнутую среду, обеспечивающую контроль целостности ПО и допускающую работу пользователей строго в рамках, предоставляемых им возможностей и полномочий.

11. Периодически контролировать неизменность (целостность) файлов, используемых для работы СКЗИ «Крипто-КОМ 3.4», входящего в состав Системы «iBank» и файлов его среды исполнения.

11.1. Для контроля неизменности файлов используется утилита rush.exe, размещенная на сайте Банка в сети Интернет https://ibank.thbank.ru.

11.2. Контрольные суммы, вычисленные утилитой rush.exe для контролируемых файлов, следует сравнивать с эталонными.

11.3. Для контроля неизменности файлов среды исполнения СКЗИ «Крипто-КОМ 3.5» необходимо сформировать список файлов для контроля целостности и рассчитать значения их контрольных сумм. При каждом обновлении операционной системы следует обновить список файлов для контроля целостности и скорректировать значения их контрольных сумм.

11.4. В «Инструкции по контролю целостности СКЗИ «Крипто-КОМ 3.5» и его среды исполнения», размещенной на сайте Банка в сети Интернет https://ibank.thbank.ru, содержится информация:

– о форматах запуска утилиты rush.exe в режиме вычисления контрольных сумм и в режиме контроля целостности файлов;

– о составе файлов среды исполнения для поддерживаемых СКЗИ «Крипто-КОМ 3.5» операционных систем, неизменность которых следует контролировать;

– об эталонных значениях контрольных сумм файлов СКЗИ «Крипто-КОМ 3.5», неизменность которых следует контролировать.