РЕКОМЕНДАЦИИ
по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники в целях противодействия осуществлению переводов денежных средств без согласия клиентов
ООО «Чайна Констракшн Банк»

Москва
2025

1. Общие положения

Настоящий документ разработан ООО «Чайна Констракшн Банк» (далее – Банк) в соответствии с требованиями Положения Банка России от 30.01.2025 №851-П «Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

Настоящий документ определяет:

– рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее – вредоносный код) в целях противодействия осуществлению переводов денежных средств без согласия клиента;

– возможные риски получения несанкционированного доступа к защищаемой информации с целью совершения действий в целях осуществления банковских операций лицами, не обладающими правом на их совершение, и мерах по снижению указанных рисков:

- мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) компьютера (ноутбука), с использованием которого клиентом совершались действия в целях осуществления банковской операции;
- мерах по контролю конфигурации компьютера, с использованием которого клиентом совершаются действия в целях осуществления банковской операции, и своевременному обнаружению воздействия вредоносного кода.

2. Рекомендации по защите информации от воздействия вредоносного кода

На компьютере (ноутбуке), который предназначен для работы с системой дистанционного банковского обслуживания (далее – компьютер), необходимо использовать следующие средства защиты от воздействия вредоносного кода:

- средство защиты от вредоносного кода (далее – антивирус);
- средство межсетевого экранирования;
- средство предотвращения/обнаружения вторжений;

- иные средства защиты информации.

Не используйте права администратора на компьютере при отсутствии необходимости. В повседневной практике входите в систему дистанционного банковского обслуживания с учетной записью пользователя, не имеющего прав администратора.

Устанавливайте на компьютер программное обеспечение только из доверенных источников, которое требуется только для функционирования системы дистанционного банковского обслуживания.

В случае подозрения на заражение компьютера вредоносным кодом, следует незамедлительно отключить компьютер от сети и сообщить об этом в Банк, а также предпринять действия по перевыпуску ключа электронной подписи.

Своевременно устанавливайте обновления системного и прикладного программного обеспечения, а также средств защиты информации.

Доступ к сети Интернет на компьютере должен быть ограничен: должны быть доступны только ресурсы для доступа к системе дистанционного банковского обслуживания, а также ресурсы для получения обновлений системного и прикладного программного обеспечения, обновления средств защиты информации.

3. Возможные риски получения несанкционированного доступа к защищаемой информации

Основной и самый критический риск несанкционированного доступа к защищаемой информации – получение доступа к системе дистанционного банковского обслуживания с последующими действиями, связанными с переводом денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.

4. Меры по предотвращению несанкционированного доступа к защищаемой информации

Никогда не передавайте третьим лицам информацию, которую они могут использовать для несанкционированного доступа к защищаемой информации. К такой информации относятся сведения об:

- адресах расположения ресурсов системы дистанционного банковского обслуживания в сети Интернет,
- используемых мерах и способах защиты информации в системе дистанционного банковского обслуживания,

- принятых процедурах подключения к системе дистанционного банковского обслуживания, хранения, использования носителя ключа электронной подписи и т.п.

Не храните реквизиты доступа к системе дистанционного банковского обслуживания в открытом виде, в файлах на компьютере, не используйте функцию «Запомнить пароль» при работе с системой дистанционного банковского обслуживания.

Вставляйте носитель ключа электронной подписи в компьютер непосредственно перед началом работы в системе дистанционного банковского обслуживания. Обязательно извлекайте из компьютера носитель ключа электронной подписи сразу после завершения работы с системой дистанционного банковского обслуживания.

Осуществляйте информационное взаимодействие с Банком, используя контактные данные, которые указаны в документах, полученных непосредственно от Банка.

Если в процессе работы вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет вам войти в систему, необходимо как можно быстрее обратиться в Банк для получения инструкций по смене пароля.

Незамедлительно информируйте Банк при получении информации (СМС, электронных писем, телефонных звонков от имени Банка), связанной с системой дистанционного банковского обслуживания Банка, которую Вы не ожидаете получить.

Сотрудники Банка никогда не попросят у вас реквизиты доступа к системе дистанционного банковского обслуживания. Если вам поступил звонок, в котором собеседник представился сотрудником Банка и просит у сообщить ему реквизиты доступа к системе дистанционного банковского обслуживания, следует прервать разговор, перезвонить в Банк самостоятельно и сообщить об этом событии.

Необходимо блокировать компьютер, когда не осуществляется работа в системе дистанционного банковского обслуживания. Ограничьте возможность использования съемных носителей информации на компьютере.

Принимайте меры по исключению доступа посторонних лиц в помещения, в которых размещены компьютеры для работы с системой дистанционного банковского обслуживания.

5. Меры по контролю конфигурации компьютера, с использованием которого совершаются действия в целях осуществления банковских операций

Для контроля конфигурации компьютера для работы с системой дистанционного банковского обслуживания необходимо использовать специализированные средства защиты информации.

6. Заключительные положения

Рекомендации, перечисленные в настоящем документе, не следует рассматривать как исчерпывающий перечень мер защиты информации, исполнение которых позволит полностью исключить риск инцидентов информационной безопасности.

Обязанность внесения изменений в настоящий документ вследствие изменения действующего законодательства Российской Федерации, нормативных документов Банка, изменения регламентов и процедур возлагается на Отдел информационной безопасности.

Документ подлежит регулярному пересмотру в соответствии с требованиями, предусмотренными документом РР3-ICS-008 Инструкция по работе с внутренними нормативными документами Банка.

Документ доводится до клиентов Банка посредством размещения на официальном сайте Банка.