

Рекомендации по обеспечению безопасной среды для использования систем интернет-банкинга

Для снижения рисков, возникающих при осуществлении операций с применением систем интернет-банкинга, рекомендуем руководствоваться следующими правилами:

1. Строго сохраняйте в тайне закрытый (секретный) ключ электронно-цифровой подписи (ЭЦП). Для этого:

- храните носители, содержащие ключевую информацию (далее, носители) и их дубликаты в сейфе;
- покидая рабочее место всегда извлекайте носители и помещайте их в место хранения;
- не допускайте работу других пользователей за автоматизированным рабочим местом, на котором загружена ключевая информация.

2. В случаях компрометации или подозрения на компрометацию ключей ЭЦП, а также по истечению срока их действия требуется их незамедлительная замена. К событиям, связанным с компрометацией ключей, относятся, в том числе, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение целостности печатей на сейфах с ключевыми носителями, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей с последующим обнаружением;
- доступ посторонних лиц к ключевой информации.

3. По истечению срока действия ключа необходима его замена.

4. Запрещается использование ключей ЭЦП и другой аутентификационной информации при доступе к системе интернет-банкинга с гостевых и публичных рабочих мест (интернет-кафе и т. д.) в связи с высоким риском хищения и дальнейшего неправомерного использования ключа ЭЦП.

5. Пользуйтесь антивирусным программным обеспечением и своевременно обновляйте антивирусные базы.

6. Своевременно обновляйте компоненты операционной системы и используемого программного обеспечения (Microsoft Internet Explorer, Mozilla FireFox, Opera, Google Chrome, Apple Safari, Nullsoft Winamp, RealNetworks Real Player, Adobe Flash Player и др.)

7. Ни в коем случае не открывайте вложения в письмах, пришедших вам по электронной почте от имени Банка или его сотрудников, не переходите по ссылкам, указанным в таких письмах.

8. Ни в коем случае не передавайте идентификационную и ключевую информацию третьим лицам. Банк никогда не просит предоставить такую информацию. О любом таком случае сообщайте по телефону (343) 378-78-78.

Термины и определения, применяемые в данной рекомендации

Под субъектом понимается пользователь, осуществляющего доступ к интернет-банкингу.

Систем идентификации и аутентификации – система, задачей которой является определение и верификация набора полномочий субъекта при доступе к интернет-банкингу.

Идентификация субъекта при доступе к интернет-банкингу – процесс сопоставления его с некоторой хранимой системой характеристикой субъекта – идентификатором. В дальнейшем идентификатор субъекта используется для предоставления субъекту определенного уровня прав и полномочий при использовании информационной системой.

Аутентификацией субъекта называется процедура верификации принадлежности идентификатора субъекту.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

Закрытый ключ ЭЦП – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах ЭЦП с использованием средств ЭЦП;

Компрометация ключа – утрата доверия к тому, что используемые закрытые ключи недоступны посторонним лицам.