Российская Федерация
Муниципальное казенное учреждение
«Централизованная бухгалтерия
города Усолье-Сибирское»
(МКУ «ЦБ г. Усолье-Сибирское»)

ПРИКАЗ

19.12.2017г. № 340

г. Усолье-Сибирское

« Об утверждении политики
обеспечения безопасности
платежных систем
МКУ «ЦБ г. Усолье-Сибирское»

В целях исполнения законодательства Российской Федерации в области обеспечения информационной безопасности

ПРИКАЗЫВАЮ:

1. Утвердить политику обеспечения безопасности платежных систем в МКУ «ЦБ г. Усолье-Сибирское» (Приложение №1).
2. Заместителю директора Левиной О.А. организовать размещение данного приказа на странице официального сайта МКУ «ЦБ г. Усолье-Сибирское».
3. Инспектору по кадрам Спешиловой Т.Н. организовать ознакомление сотрудников МКУ «ЦБ г. Усолье-Сибирское», в том числе вновь поступающих на работу с настоящим приказом.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МКУ «ЦБ г. Усолье-Сибирское» Л.Ф.Шевнина

Приложение № 1
к приказу МКУ «ЦБ
г.Усолье-Сибирское»
от 19.12.2017г. № _340_

Политика
обеспечения безопасности платежных систем
МКУ «ЦБ г. Усолье-Сибирское»

1. Термины и определения

Аутентификация - подтверждение подлинности и достоверности.
Доступность - свойство системы (средств и технологий обработки, инфраструктуры в которой циркулирует информация), которое характеризует способность обеспечивать своевременный доступ субъектов к интересующей их информации и соответствующим автоматизированным службам.
Информационная безопасность (ИБ) - обеспечение конфиденциальности, целостности и доступности информационных ресурсов (активов) Банка, а также аутентичности данных и отказоустойчивости.
Информационные ресурсы (активы) - информационные ресурсы (активы) Банка включают в себя информацию, напечатанную или записанную на бумаге, пересылаемую по почте или демонстрируемую в видеозаписях, передаваемую устно, хранимую в электронном виде на серверах, web сайтах, мобильных устройствах, магнитных и оптических носителях и т.п., а также обрабатываемую в корпоративных информационных системах и передаваемую по каналам связи.
Информационные ресурсы Банка также включают в себя программное обеспечение:
операционные системы, приложения, утилиты, программную документацию и т.п.
Конфиденциальность - доступность информации только для авторизованных пользователей.
Нарушение безопасности - любые действия, которые влекут за собой (или могут повлечь) нарушение доступности, конфиденциальности или целостности информационных ресурсов Банка, а также аутентичности или отказоустойчивости.

целостности информационных ресурсов Банка, а также аутентичности или отказоустойчивости.

Обеспечение информационной безопасности - защита информации от широкого спектра угроз (в отношении конфиденциальности, целостности, доступности, аутентичности и отказоустойчивости) с целью обеспечения непрерывности бизнеса, минимизации бизнес рисков, максимизации прибыли на инвестированный капитал и получения дополнительных возможностей для бизнеса.

Отказоустойчивость - способность сетевого устройства, его модулей предотвращать ошибки или восстанавливаться после сбоев.

Целостность - достоверность и полнота информации и методов ее обработки, а также отсутствие несанкционированных изменений информации.

2. Требования по обеспечению безопасности платежных систем

2.1. Требования по обеспечению безопасности платежных систем, а также банковского информационного технологического процесса должна соответствовать требованиям настоящей Политики.

Банковский платежный технологический процесс должен быть документирован.

2.2. Должны быть документально определены перечни программного обеспечения, устанавливаемого и (или) используемого в ЭВМ и необходимого для выполнения конкретных банковских платежных технологических процессов.

2.3. Комплекс мер по обеспечению ИБ банковского платежного технологического процесса должен предусматривать в том числе:

– защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений;

– доступ сотрудника только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;

– контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;

– аутентификацию входящих электронных платежных сообщений;

– двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями;

– возможность ввода платежной информации только для авторизованных пользователей;

– контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.);

– восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;

– сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов;

– доставку электронных платежных сообщений участникам обмена.

При эксплуатации систем дистанционного банковского обслуживания должны быть документально определены и выполняться процедуры, реализующие в том числе механизмы:

– снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами;

– доведения информации о возможных рисках, связанных с выполнением операций или транзакций до клиентов.

Должны быть документально определены процедуры обслуживания средств вычислительной техники, используемых в банковском платежном технологическом процессе, включая замену их программных и (или) аппаратных частей.

3. Ответственность

Сотрудники Учреждения несут ответственность по действующему законодательству за разглашение сведений ограниченного распространения, ставших им известными в результате работы. Любое грубое нарушение порядка и правил работы в корпоративной сети сотрудниками должно расследоваться.

К виновным должны применяться адекватные меры воздействия.

Нарушение установленных правил и требований по обеспечению информационной безопасности являются основанием для применения к сотруднику административных мер наказания, вплоть до увольнения и привлечения к уголовной ответственности.