Обеспечение Безопасности Системы HandyBank

ЗАО «ХэндиСолюшенс» одновременно является и разработчиком программных средств Системы HandyBank и оператором Системы HandyBank, оказывающим банкам-участникам услуги по информацинно-технологическому взаимодействию.

Как организация - разработчик программного обеспечения ЗАО «ХэндиСолюшенс» сертифицировано на соответствие требованиям стандарта ISO 9001:2008 – Системы менеджмента качества. Требования.

Как организация, оказывающая информационно-технологические услуги, ЗАО «ХэндиСолюшенс» сертифицировано на соответствие требованиям стандарта ISO/IEC 27001:2005 – Стандарт информационной безопасности.

Как организация, хранящая и обрабатывающая информацию, содержащую данные банковских карт, ЗАО «ХэндиСолюшенс» сертифицировано на соответствие требованиям стандарта PCI DSS - Payment Card Industry Data Security Standard.

В ходе ежегодных прохождений вышеуказанных сертификаций, а также с установленной периодичностью между сертификациями, ЗАО «ХэндиСолюшенс» подвергается всесторонним проверкам и обследованиям со стороны соответствующих уполномоченных сертифицирующих организаций.

Такие проверки включают в себя не только установление соответствия внутренних правил и процедур ЗАО «ХэндиСолюшенс» этим стандартам, но и полномасштабное тестирование информационных систем, включая попытки внешнего взлома и несанкционированного проникновения в информационные системы.

Безопасность функционирования Системы HandyBank, включая защиту от совершения операций неуполномоченными лицами, обеспечивается также следующим:

1. При совершении операций никакие реквизиты банковских карт не передаются через Интернет;
2. Доступ пользователей к сайту системы осуществляется с использованием протокола HTTPS/SSL, обеспечивающим защиту всей передаваемой информации от несанкционированного доступа (шифрование);
3. При осуществлении входа в систему (логин/пароль) принимаются меры по предотвращению попыток подбора пароля (антиподбор), а при установлении (смене) пароля происходит тест на достижение паролем определенной степени сложности;
4. По желанию пользователя для предотвращения перехвата пароля вредоносными резидентными программами может использоваться виртуальная клавиатура;
5. Для подтверждения операций в Системе HandyBank реализованы два способа авторизации, каналы доставки которых физически отделены от канала формирования операции:
    a. Авторизация с использованием SMS-сообщения;
    b. Авторизация с использованием генератора одноразовых паролей (токена) 2-го поколения.
6. По желанию пользователя может также осуществляться вход в систему с использованием указанных средств авторизации.

Риски клиентов, связанные с проведением операций в Системе HandyBank, застрахованы компанией «Росгосстрах» с лимитом 3 млн. рублей по одному страховому случаю.