Михаил Левашов, профессор НИУ ВШЭ

Кибербезопасность – это не обязательно дорого

Нас к этому приучают, поэтому мы уже привыкли, что обеспечение кибербезопасности это - достаточно дорогое и сложное дело. Действительно, даже по самым скромным рекомендациям, а также требованиям регуляторов (ФСТЭК и ФСБ) необходимо приобрести, установить и настроить оборудование и программное обеспечение (далее ПО), которое позволит защититься от вирусного ПО и утечки данных (DLP и криптография). Необходимо использовать системы управления учётными записями и доступом (IDM), учёта угроз и информационной безопасности (далее - ИБ). И так далее и тому подобное. Читатель уже напуган большим объемом работ и большими расходами. Торопимся успокоить его: на самом деле не все так сложно и дорого! В некоторых наиболее часто встречающихся в жизни ситуациях, особенно касающихся финансовой сферы, можно простыми организационными мерами свести риски нарушений (хищений средств) практически к нулю.

Речь идёт о проведении платежей через различные системы интернет банкинга. Это могут быть платежи предприятий, осуществляемые работниками бухгалтерий или другими уполномоченными лицами, а также платежи физических лиц. Рассмотрим один конкретный случай.

Итак имеем автоматизированную систему интернет банкинга (далее - АС), клиентский модуль которой установлен на стационарном компьютере, либо на мобильном устройстве. Если вход в АС осуществляется через web интерфейс, то клиентским модулем является, по сути, любой интернет браузер (тонкий клиент), установленный на компьютере или мобильном устройстве. Будем также преподавать, что АС использует для подтверждения операций СМС уведомление. В настоящее время это - наиболее часто применяемая технология.

Для минимизации риска нарушений (хищений) необходимо использовать как минимум два устройства. С одного устройства вы заходите в АС для проведения транзакции, на другое устройство приходит СМС для подтверждения транзакции. При этом это второе устройство может быть дешевым кнопочным мобильным телефоном. Далее, при частом использовании этой технологии, то есть, при большой частоте поведения транзакций необходимо также часто менять пароли на вход в АС. Лучше делать это каждый день. При небольшом количестве транзакций (например, несколько раз в месяц) рекомендуется менять пароль после каждой транзакции. Важно отметить, что процедуру смены пароля нужно производить на 3-м независимом от первых двух устройстве, например, в банкомате. Предполагается, что АС допускает такую технологию.

Заметим, что при такой организации платежей вероятность их компрометации или хищения денежных средств будет практически равна нулю. Причём это утверждение верно и в случае заражения одного или обоих используемых устройств вирусным ПО. При этом частая смена паролей - очень важная особенность такой простой технологии. Важность такой смены паролей недавно на прошедшем в Москве международном конгрессе по кибербезопасности отметил руководитель Сбербанка Г. Греф.