



Ассоциация
Российских
Банков

ВЫСТУПЛЕНИЕ НА IX УРАЛЬСКОМ ФОРУМЕ “ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВОЙ СФЕРЫ”

Гарегин Тосунян

14 февраля 2017г.



ТЕЗИС 1.

Комитет АРБ по банковской безопасности проанализировал многие «законы», «указы», «стратегии», «постановления» и другие «нормативно-правовые» документы разного уровня, в которых прописана «правовая ответственность» подразделений информационной безопасности банков. Выяснилось, что общее количество таких документов около 130:

- федеральных законов – порядка 50;
- указов Президента и постановлений Правительства – более 20;
- актов федеральных органов исполнительной власти – около 15;
- нормативных документов Банка России – порядка 25;
- стандартов и нормативных документов по международным (ВИЗА, МАСТЕРКАРД и др.) и российским (НСПК и др.) платежным системам, а также по международной системе совершения платежей СВИФТ – более 20.

ТЕЗИС 2.

Назрела необходимость в упорядочении этих документов и в создании, по возможности, единого отраслевого документа по информационной безопасности, позволяющего кредитно-финансовым организациям оперативно реагировать на постоянно возникающие новые вызовы.



ТЕЗИС 3.

Целеполагание, прогнозирование, планирование и программирование в обеспечении информационной безопасности позволят, безусловно, упорядочить нашу совместную деятельность.

В связи с этим предлагается создать Стратегию развития информационной безопасности организаций кредитно-финансовой сферы.

ТЕЗИС 4.

Для наиболее эффективного использования потенциала банковского сообщества при подготовке Стратегии, необходимо привлечь к участию все заинтересованные организации, и предложить Банку России возглавил этот процесс в качестве межведомственного координатора. Что касается постановки целей, задач, критериев и прочее при подготовке Стратегии, то будет полезно и эффективно объединить наработанный опыт Банка России по подготовке и реализации подобных проектов с потенциалом профессионального банковского сообщества.



ТЕЗИС 5.

Отсутствует механизм срочной блокировки мошеннических сайтов с иностранными доменами.

Российские регистраторы, по-прежнему, не несут никакой ответственности за регистрируемые ими сайты.

Все это позволяет мошенникам оставаться практически безнаказанными.

В основном мошеннические сайты используются:

- для сбора персональных данных (фишинг);
- для кражи денежных средств владельцев банковских карт и иных электронных средств платежа.

ТЕЗИС 6.

Назрела необходимость в решении острой проблемы, связанной с отсутствием механизмов срочной блокировки мошеннических сайтов.

Считаем необходимым в срочном порядке создать Межведомственную рабочую группу, в состав которой кроме специалистов банковского сообщества должны войти представители силовых ведомств,

Минкомсвязи, Роскомнадзор, а также все заинтересованные организации.



Ассоциация
Российских
Банков



Ассоциация
российских
банков

www.arb.ru

Спасибо за внимание!