О секретных нарушениях банков

Если человек хочет рассказать о наболевшем миру, он пишет пост в соцсетях. Департамент информационной безопасности ЦБ в такой же ситуации пишет секретное письмо с грифом «для служебного пользования» поднадзорным банкам и отправляет строго по защищенным каналам связи, ведь в нем вся печаль и боль регулятора.

Одно из подобных писем от департамента информационной безопасности ЦБ банки получили 16 апреля. В письме регулятор привел типичные нарушения, выявленные при проверках в первом квартале 2019 года: тут и закон «О национальной платежной системе» 161-ФЗ в части необеспечения защиты информации, и закон «О банках и банковской деятельности» в части банковской тайны, и положение ЦБ №382-П с перечислением множества пунктов с указаниями нарушений.

Есть тут и отсутствие средств защиты от вредоносного кода, отсутствие контроля программного обеспечения, отсутствие регистрации прав доступа к защищаемой информации и т. д. Кроме того, были отмечены нарушения работы со средствами криптографической защиты, идентификации, аутентификации, недостаточный внутренний контроль информационной безопасности, отсутствие антивирусов.

После длинного перечня ссылок на разные нормативные акты с указанием нарушений ЦБ приходит к прискорбному выводу, что выявленные нарушения связаны «с человеческим фактором», а именно: недостаточными знаниями и ответственностью специалистов по информбезопасности, формальным отношением собственников и руководителей банков к этим вопросам. И неутешительный вывод: нарушения могут привести к реализации операционного риска, в том числе хищению денежных средств.

В ЦБ пояснили «Ъ», что документ является «методологическим», банки должны использовать его в работе. Однако опрос поднадзорных показал, что никакой полезной информации или рекомендаций они для себя не вынесли. Одни увидели в письме скрытую угрозу типа «ЦБ знает о ваших проделках», другие шутили, что регулятор привел типовой перечень «косяков», чтобы в банках не переживали: их ошибки не являются исключением.

А нам кажется, что письмо просто крик души регулятора. Ну посудите сами: требования нормативных документов банки не выполняют, специалисты ничего не знают, к информационной безопасности относятся формально. При этом штрафных санкций за нарушение информационной безопасности нет, киберриски будут входить в операционный риск и влиять на капитал не раньше следующего года. Вот и остается ЦБ высказывать свою печаль в письмах под грифом, поскольку безопасность любит тишину.

(www.kommersant.ru)