BIS JOURNAL
информационная безопасность банков

Игорь ХАЙРОВ
проректор
Академии
Информационных Систем

Дмитрий ЛЕВИЕВ
эксперт по безопасности
Академии
Информационных Систем,
председатель правления
НП «ПСИБ»

И УЧИТЬСЯ, И УЧИТЬ

РАБОТА НАД ОБУЧАЮЩИМИ ПРОГРАММАМИ – НЕ ТРАТА ВРЕМЕНИ И СРЕДСТВ, НО ИНВЕСТИЦИИ В БЕЗОПАСНОЕ БУДУЩЕЕ?

Небольшой мир учебных центров в области информационной безопасности и информационных технологий сейчас переживает серьезные изменения: с 1 сентября 2013 года согласно закону №273-ФЗ «Об образовании в Российской Федерации» все образовательные учреждения, реализующие программы дополнительного профессионального образования, лишатся возможности выдавать дипломы государственного образца. С одной стороны, это проблема. Но скорее самих учебных центров. Специалисты же банковской сферы, приходящие в Академию Информационных Систем, нуждаются не в «корочке», по их личному замечанию, а в реальных знаниях, практиках и экспертизе.

Поэтому нам интересно было бы поговорить о роли образования в рамках нового закона 161-ФЗ «О национальной платежной системе» и Постановления 382-П. Причем, начиная разговор об обучении в этот раз, мы видим банковское сообщество в роли наших коллег.

НА СТЫКЕ ИНТЕРЕСОВ

Вся современная платежная система функционирует на стыке интересов трех сторон: регулятора, банка и клиента. При этом, в процессе взаимодействия каждый из участников преследует свои интересы, часто эти интересы взаимоисключают друг друга. Сегодня для клиента важно удобство пользования банковскими системами и скорость реализации платежей. К сожалению, удобная оплата «в один клик» может обернуться неприятными последствиями для клиента, если все участники платежной цепочки не предприняли необходимых мер безопасности при обработке данных.

Безопасность хранения денежных средств на счетах клиентов хоть и является для бизнеса вопросом репутации, но прямой выгоды, скажем честно, не несет. Именно поэтому в игру вступают государственные регуляторы и международные сообщества, устанавливающие требования к защите. Однако чтобы не случилось перекоса в какую-то одну из сторон требования должны быть адекватными к исполнению, что можно достичь только при тесном сотрудничестве в написании нормативных документов.

Глобальная задача, стоящая перед сообществом участников ПС, – это поиск консенсуса в вопросах «что хочет регулятор», «что может и хочет делать банк» и «что может и согласится исполнить клиент». В случае достижения этого консенсуса нам удастся построить эффективную систему безопасных платежей, работающую на единой методологической платформе.

ОТ «МЯГКОГО» К ОБЯЗАТЕЛЬНОМУ

Понятно, что идея обеспечения безопасности платежей не нова: Банк России совместно с банковским сообществом уже давно разработали комплекс стандартов СТО БР ИББС. Это был большой рывок вперед в области регулирования отношений в банковской отрасли, сопровождаемый сложно решаемыми вопросами. Но впрочем, о них позже.

Первая редакция Стандарта вышла в 2004 году. И сообщество сразу же столкнулось с проблемой отсутствия единой методики внедрения и аудита выполнения требований в банках. В 2006 году Академия Информационных Систем запустила единственную на рынке линейку курсов, согласованную с Советом Сообщества ABISS: введение в СТО БР ИББС, внедрение Стандарта, внутренний и внешний аудит выполнения требований Стандарта. Важно: методологию обучения и программы курсов создавали в АИС при участии непосредственных разработчиков Стандарта Банка России, они же и проводили обучение и проводят его до сих для слушателей Академии.

Цель данной линейки курсов заключалась в изучении принципов и подходов к обеспечению информационной безопасности в организациях БС РФ на основе положений и рекомендаций Стандарта Банка России, овладение практическими приемами построения эффективной системы обеспечения информационной безопасности, основанными на опыте внедрения Комплекса Стандартов Банка России в кредитно-финансовых учреждениях РФ.

Обучение по единой методологии всех участников – сотрудников банков, интеграторов, аудиторов (но не клиентов) – дало положительный результат в становлении и популяризации Стандарта. Но из-за явных противоречий с действующими на тот момент законами, в частности с законом «О персональных данных» банки не спешили приводить свои системы в соответствие с необязательными, а только лишь рекомендательными требованиями СТО БР ИБСС.

Однако в последние несколько лет законодательство в банковской отрасли существенно продвинулось. С появлением в 2012 году закона «О национальной платёжной системе» ЦБ РФ, по согласованию с ФСБ России, ФСТЭК России и Минюстом РФ, выпустил Положение 382-П, которое в отличие от СТО БР ИББС стало обязательным к исполнению. Так, в достаточно сложной ситуации оказались банки, не занимавшиеся приведением своих систем в соответствие с требованиями ЦБ РФ. Однако их не так много, сообщил ЦБ РФ, в конце прошлого года – не более 20% от всех кредитно-финансовых организаций.

Тем не менее, с появлением новых требований необходимо разрабатывать новую методологию для всех участников платежного процесса. Оглядываясь на предыдущий опыт работы в рамках Стандарта, сообщество прекрасно понимает, что грамотно и эффективно организовать защиту информации при денежных переводах и добиться прозрачности оценки можно только при наличии соответствующих единых, универсальных требований и единой методологии внедрения и контроля.

ВЫ – САМОЕ СЛАБОЕ ЗВЕНО. УЧИТЕСЬ!

Мы уже выяснили, что в работе современной платежной системы должны учитываться интересы трех сторон: регулятора, бизнеса (банка) и клиента. Стоит ли говорить, что в этой цепочке наиболее уязвимое место – это клиентская сторона. Еще в рамках конференции «Борьба с мошенничеством в сфере высоких технологий. Профилактика и противодействие. AntiFraud Russia – 2012», подвели неутешительный итог: к каким бы надежным средствам защиты не прибегали банки, как бы строго их не контролировал регулятор, все впустую, если клиент не владеет хотя бы элементарными знаниями и навыками защиты своих данных и денежных средств на счету.

Общая грамотность пользователей банковскими услугами находится на крайне низком уровне, что является благодатной почвой для роста уровня мошенничества в финансовой отрасли и большой проблемой для кредитно-финансовых учреждений. Кто из среднестатистических клиентов знает о том, как распознать – легальный ли банкомат перед ним или нет? Кто из них внимательно обращает внимание на адресную строку в момент совершения онлайн-платежа?

Этого не делают, потому что не подозревают о подстерегающих их опасностях. Проблема общей грамотности (читай – безграмотности) населения – это проблема Минобрнауки РФ, можете возразить вы. Даже если предположить, что в Министерстве образования и науки возьмутся за этот вопрос сегодня, когда стоит ждать результатов? 7, 10 лет? Ответ однозначный, сообщество столько ждать не может.

Логичным выходом из текущей ситуации станут несколько последовательных шагов. Во-первых, интересы и обязанности клиентов должны быть учтены в процессе разработки единой методологии внедрения, оценки в соответствии Положению 382-П.

Во-вторых, проведение неоднократных обучающих мероприятий для всех пользователей банковских услуг. Задача этого шага – приведение в порядок «средней температуры по больнице». А следующим, третьим шагом должно стать внедрение специальных, уникальных образовательных программ банков для их клиентов с учетом специфики методов защиты информации конкретным банком. Причем работу в этом направлении для кредитно-финансовых организаций проще и менее затратно отдать на разработку учебным центрам, имеющим в преподавательском составе экспертов, участвующих в разработке единой методологии.

***

Популяризация идеи защиты информации и денежных переводов среди обычных пользователей – это не менее важный аспект, который должен быть реализован в рамках Национальной платежной системы, чем внедрение систем защиты и написание требований. Работа над обучающими программами – это не трата времени и средств, но инвестиции в безопасное будущее.