

свои карты и счета, все операции онлайн детям и внукам.

Александр Цапко. А потом пенсионер приходит в банк с вопросом: «Где мои деньги?..»

Сергей Нечаев. С другой стороны, пенсионеры в любом случае попадают в целевую аудиторию интернет-технологий. Ведь интернет не подразумевает выход из дома, что является положительным моментом для тех, кому физически сложно дойти до банка.

Александр Бродерзон. Да, если смотреть по возрастным категориям, то мы увидим примерно такие цифры: среди клиентов до 30 лет охват интернет-сервисом составляет 100%, 30–50 лет — 70%, от 60 и выше — уже всего около 5%. Но как уже говорилось, когда мы все попадем в категорию «после 60», эта доля существенно увеличится.

Артем Маслов. Иными словами, последний офис обслуживания умрет вместе с нами.

В БОРЬБЕ ЗА БЕЗОПАСНОСТЬ

Сергей Нечаев. Я хотел бы поднять еще такой вопрос: с развитием интернет-

заботиться о безопасности. Потому что если хотя бы один банк разработал некачественное ПО для работы в интернете, эта информация быстро распространяется, и у людей доверие теряется. Плюс банки должны всегда помнить о том, что они ответственны и за обучение своих клиентов правилам безопасной работы.

Андрей Федоров. А как в практической плоскости построена эта работа сегодня?

Артем Маслов. Прежде всего, это индивидуальная работа. Мы пытаемся убеждать в необходимости приобретать средства дополнительной защиты, чтобы клиент больше внимания уделял санации и профилактическим мерам относительно своего рабочего места. На деле очень часто сталкиваемся с непониманием в отношении этого. Наверное, это пока показатель общей культуры, потребители услуг в основной массе еще не дошли до этого уровня сознательности.

Алексей Кистанов. Безопасность — один из самых кардинальных вопросов, с которыми

наглядно: есть банки, а есть «наперсточники», и они далеко друг от друга дистанцированы. В интернете все оказывается рядом. Банк, хороший интернет-магазин, а рядом... «наперсточник».

Алексей Кистанов. Некоторые сознательно идут на рискованные сайты. К примеру, много любителей интернет-казино.

Сергей Нечаев. Действительно, появилось много таких транзакций после того, как запретили игровой бизнес. Причем нередко транзакции приходят из интернет-казино, сервер которых расположен в других государствах.

Александр Цапко. После того как на всех картах появился чип, защита стала гораздо серьезнее. В частности, появилась возможность использовать электронно-аппаратное устройство для получения одноразового пароля. Это гораздо лучше, чем использование пароля или электронно-цифровой подписи, как это происходило ранее с картами с магнитной полосой, потому что теперь нет необходимости иметь под рукой флешку или компьютер. Специальное устройство сто-



СЕРГЕЙ НЕЧАЕВ



АЛЕКСЕЙ БОРОДАВИН



АНДРЕЙ ФЕДОРОВ

банкинга активизируются мошенники. При помощи различных вирусных программ они воруют пароли, компрометируют данные кредитных карт. Представителям крупных банков на самом деле известно, насколько небезопасна работа в интернете. Тем более что зачастую люди сами не стремятся устанавливать антивирусные программы, сообщают свои данные. И тут возникает вопрос исчезновения филиалов: а куда в таком случае сможет обратиться человек, если у него пропадут деньги со счета? Ведь он должен куда-то физически прийти, чтобы написать претензию.

Александр Бродерзон. Это вопрос действительно очень серьезный. Работая в интернете, мы от него никуда не уйдем. Мне кажется, это общая задача, глобальная для всей страны — формирование новой культуры: культуры предоставления услуг в электронном виде. Банковское сообщество в этом плане идет впереди. Однако постепенно развивается и программа «Электронная Россия», готовится к выпуску Универсальная электронная карта гражданина РФ (УЭК). То есть государство тоже идет по направлению оказания услуг в электронном виде. А тут действительно другие законы. Обязательно должны быть установлены антивирусы, должно присутствовать четкое понимание того, что нельзя никому давать свой пин-код, одноразовый пароль. Плюс сами институты — банки, государство — должны

мы сталкиваемся. Здесь очень много составляющих. Во-первых, я бы сразу разделил платежи посредством интернета и платежи с помощью веб-банка и интернет-банка. Это разная степень безопасности. Если человек заходит на веб-банк, сайт которого поддерживает сам банк, уровень защиты на порядок выше. Я вообще не слышал, чтобы были проблемы в таких ситуациях. Если клиент оплачивает услуги в интернет-магазине, введя номер своей карты, то за безопасность отвечает владелец сайта, с которым у клиента нет никаких отношений. Как правило, у части пользователей есть смешение этих понятий. Наша задача — в первую очередь научить различать разные способы и механизмы оплаты. Далее, если говорить о веб-банке, то дифференцируются различные формы оплаты. Мы рекомендуем клиентам для оплаты через веб-банк приобретать отдельную банковскую карту. Как вариант, она может быть виртуальной.

Екатерина Рябенко. Мы тоже своих клиентов обучаем тому, что, если они расплачиваются в интернете, не надо афишировать счет своей дебетовой карты. Лучше открыть виртуальную карту с лимитированной суммой.

Алексей Кистанов. Более того, можно на определенный период, когда вы регулярно совершаете платежи, при помощи мобильного банка включить разрешение операций по карте. А потом запретить.

Александр Бродерзон. Тут еще такой момент. Получается, что в обычной жизни очень

ит недорого, но позволяет кроме компьютера пользоваться интернет-банкингом еще и с мобильного телефона. Учитывая, что в России 30 млн пользователей интернета, а мобильных телефонов зарегистрировано намного больше, чем жителей, это очень перспективное направление.

Александр Бродерзон. Действительно, например, если мы говорим об электронной карте гражданина, необходимо ЭЦП, и единственно понятный способ его хранения — чип. То есть наличие чипа — необходимое требование к универсальной карте гражданина. А чтобы чип прочитать, необходимо использовать специальные устройства. Так что если все органы государственной власти вместе с банками и другими коммерческими организациями будут работать на единую цель, это станет нормой и, естественно, представит уже другой уровень безопасности. Однако одному банку внедрить это достаточно тяжело.

Андрей Федоров. Какие действия предпринимает банк в случае мошенничества?

Артем Маслов. Я с коллегами согласен — банковская система ушла в этом направлении далеко вперед. А вот система правоохранительных органов не готова к такому виду мошенничества, не готова обрабатывать их в массовом, системном порядке, несмотря на то что за 6 месяцев 2010 года было зарегистрировано около 1,5 тысячи несанкционированных доступов к счетам юридических лиц. По сути, такие дела