О ЧИСЛЕННОЙ ОЦЕНКИ УЯЗВИМОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-БАНКИНГА

Найденова Д.Р.
Научный руководитель – д.т.н., проф. Антипов И.Е.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Науки, 14, кафедра КРиСТЗИ, (057) 702 14 30
e-mail: diana.naidonova@nure.ua, тел.: (095) 416 55 37

With each payment on the Internet, we disclose our personal data. This may pose a risk for possible fraud. To assess this risk and the effectiveness of protective measures, a numerical vulnerability assessment is needed. Abstracts on the numerical assessment of the vulnerability of personal data, by analogy with the credit rating. Factors to consider are indicated.

В настоящее время развитие информационных технологий способствует активному и повсеместному внедрению интернет–банкинга. Это вызвано как объективными причинами (удобство, удалённость, скорость обслуживания), так и имеющим место навязыванием со стороны банковских структур, которые заинтересованы в сокращении персонала и в получении дополнительных комиссионных. Вместе с тем, сам по себе технический прогресс не делает нашу жизнь ни более счастливой, ни более безопасной. Те же информационные технологии позволяют мошенникам совершать свои действия удалённо, быстро и скрытно.

Причём, речь может идти о хищении не только денежных средств, но и персональных данных. И если о первом аспекте пользователи в большинстве своём знают, то о втором, порой, даже не подозревают.

При каждой покупке или оплате услуг в интернете мы оставляем не только формальные персональные данные (фамилия, данные банковской карты), но и многочисленные сведения о себе:

- о месте жительства, номерах телефон (при оплате счетов);
- о своих интересах, вкусах, увлечениях;
- о финансовых возможностях (категория товара, объёмы покупок);
- о состоянии здоровья (покупка лекарств, оплата медицинских услуг);
- времени отсутствия, маршрутах движения (покупка билетов, бронирование гостиниц);
- о своём окружении (заказ подарков, билетов).

Риски, обусловленные утечкой персональных данных не столь очевидны, как непосредственное хищение денежных средств. Но следует учитывать, что эти данные могут храниться сколь угодно долго и оказаться в чьих угодно руках.

Различные рекомендации по защите своих средств и персональных данных, также как и применение различных технических средств, безусловно, помогают. Но мне, как специалисту по защите информации,

важно рассмотреть эту задачу с научной точки зрения. А для этого нужно выработать механизм численной оценки уязвимости и, соответственно, эффективности тех или иных предлагаемых мер по защите.

В первую очередь необходимо оценить потенциальную уязвимость пользователя.

В качестве примера можно рассмотреть способ расчёта кредитного рейтинга клиента, который те же банки используют для оценки возможных рисков. Эти рейтинги формируются на основании нескольких параметров (история платежей, количество кредитов и т. д.), каждый из которых оценивается определённым числом и учитывается со своим весом. В результате получается число (от 300 до 850) [1], которое, как считается, определяет степень доверия и возможность банка выдать кредит данному клиенту.

По аналогии с кредитным рейтингом сформируем рейтинг уязвимости. Предполагается, что для его оценки будет использоваться 5-7 простых и очевидных параметров.

В значительной степени степень уязвимости пользователя характеризовали бы его знания психологии и действия манипуляции, а также его информированность в сфере защиты информации. К сожалению, для того, чтобы объективно оценить эти параметры, необходимо проводить полноценный экзамен. Поэтому в предлагаемом перечне параметров вместо них учитывается только пол и возраст пользователя.

Следующий параметр – наличие или отсутствие учётной записи в социальной сети. Здесь влияние двойное. Во-первых, публикуемая информация может стать доступной посторонним, а во-вторых, само наличие аккаунтов в социальных сетях предполагает стиль поведения пользователя, допускающий невнимательное отношение к персональным данным.

Непосредственно влияет на уязвимость количество оплат в интернете и количество интернет-ресурсов, на которых она производилась.

Немаловажным параметром, влияющим на уязвимость, является использование смартфона как основного гаджета пользователя. В [2] объясняется, насколько много информации может быть получено о пользователе при помощи его собственного смартфона.

Также следует учитывать частоту использования банковской карты и участие пользователя в различных рекламных акциях.

В докладе будут представлены оценки и весовые коэффициенты указанных параметров, полученные на основе данных о пользователях, пострадавших от мошеннических действий злоумышленников.

Список литературы: 1. Д.Г. Алексеева, С.В. Пыхтин, Я.М. Фальковская. Комментарий к Федеральному закону «О кредитных историях» Москва, 2006г -82 стр. 2. И. Е. Антипов, А. И. Шкарлет. «О возможности создания гибридной метеорной системы связи» Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2018. Вип. 192. С. 89–93.2018 р