БЕЗОПАСНОСТЬ ДОСТУПА К ИНФОРМАЦИИ В ПЛАТЕЖНЫХ СИСТЕМАХ

КАЦ Виктория Юрьевна
студентка факультета прикладной информатики
ПАРАСКЕВОВ Александр Владимирович
старший преподаватель кафедры компьютерных технологий и систем
ФГБОУ ВО «Кубанский государственный аграрный университет»
г. Краснодар, Россия

Статья посвящена вопросу безопасности доступа к информации пользователя, которую хранят мобильные банки. Рассмотрено понятие системы электронных платежей. Указаны требования к сохранению безопасного доступа к информации пользователя.
Ключевые слова: система электронных платежей, безопасность, пароль, информация, пользователь.

В условиях технического прогресса и развивающейся экономики появляются механизмы, которые позволяют упрощать и совершать платежные операции максимально быстро. Благодаря появлению интернет-торговли стремительно развивается система электронных платежей. Система электронных платежей, или электронная платежная система – это система расчетов между финансовыми организациями, бизнес-организациями и интернет-пользователями при покупке-продаже товаров и услуг через Интернет.

Мобильный банк – сервис, который позволяет держателям банковских карт, кредитных и дебетовых, пользоваться финансовыми услугами дистанционно. Кроме того, это система, схожая с функционалом стандартного онлайн-банкинга. Через нее можно отслеживать проведенные операции, следить за состоянием счетов, подключать финансовые услуги и пр.

Для того, чтобы повысить безопасность использования электронных платежей, при входе в учетную запись или при оплате пользователь вводит пароль. Личные пароли выбираются пользователями самостоятельно, но с учетом следующих требований:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы;

– пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

Чем сложнее пароль – тем выше безопасность доступа к данным пользователя. Сейчас приложения банков могут использовать для проверки не только набор букв и цифр, но и отпечатки пальцев, «Face id», что, кажется, гораздо проще и надежнее. У приложений мобильных банков, как и у других мобильных приложений, возникают проблемы при хранении и передаче данных. Перехватить или подобрать учетные данные для доступа можно к каждому третьему приложению. При этом плохо защищены и сервера мобильных банков: уязвимости высокой степени риска обнаруживаются в каждой исследованной системе.

Важно знать, что, если пользователь соглашается входить в мобильный банк по отпечатку пальца, приложение вынуждено сохранить на его устройстве какие-то данные, которые потом буду использованы для входа в банк. На устройстве сохранятся пароли и ПИН-коды. И если телефон будет потерян или украден, эти данные с легкостью можно будет извлечь. Однако у способа входа в приложение по отпечатку пальца или «face id» есть и плюс – ваш пароль никто не сможет подсмотреть.

Упрощенная аутентификация сделает мобильный банк удобнее, но безопаснее все-таки использовать надежный пароль. Разработчики изначально проектируют свои при-

ложения таким образом, чтобы снизить возможность хакерской атаки. Потому перед тем, как выпустить приложение или обновление к нему, разработка тщательно тестируется, в том числе на попытки взлома [1].

Удобство использования облегченной авторизации с помощью отпечатка пальца или «face id» неоспоримо. Но прежде, чем использовать такие методы для входа в приложение с данными о ваших финансах, необходимо определиться – что важнее: комфорт или безопасность.

Существует также такое понятие, как мастер-пароль. Мастер-пароль – это тип алгоритма для создания уникальных паролей воспроизводимым способом. Он используется для сохранения пользователем доступа ко всем своим учетным записям сразу. Пароли не хранятся на диске или в облаке, а каждый раз восстанавливаются на основе информации, введенной пользователем: его имени, мастер-пароля и уникального идентификатора службы, для которой предназначен пароль. Поскольку пароли нигде не хранятся, такой подход затрудняет их кражу или перехват злоумышленниками. Это также устраняет необходимость в синхронизации между устройствами, резервных копиях потенциальных баз данных паролей и рисках утечки данных. Это иногда называют управлением паролями без синхронизации. Мобильные банки содержат недостатки, которые могут привести к таким последствиям:

– утечка важных данных пользователей, включая персональные и данные банковских карт;

– несанкционированный доступ к приложению;

– проведение мошеннических операций и кража денежных средств.

Причинами могут служить некоторые из следующих факторов.

1. Ненадежный пароль. По неофициальной статистике, пароли более 30% наших сограждан состоят только из цифр, 20% – только из маленьких латинских букв, 30% – из цифр и маленьких латинских букв. И только оставшиеся 20% пользователей составляют более надежные с точки зрения информационной безопасности комбинации [2]. Если бы банки не предъявляли определенных требований к пользовательским паролям, которые мы упоминали раннее, и те были бы элементарными. 90% паролей сейчас воруются посредством фишинга, и в данном случае криптостойкость на результат никак не влияет. Однако это совершенно не значит, что нужно оставлять мошенником дополнительный шанс.

2. Вредоносные программы и фишинг. Если телефон имеет функцию выхода в интернет, то процесс его использования для обмена информацией с банком обрастает дополнительными рисками [3]. Не нужно загружать подозрительные файлы и ПО, переходить по ненадежным ссылкам.

3. Утеря устройства. Пользуясь мобильным как инструментом управления банковским счетом, нужно всегда помнить то, что устройство может быть утеряно. Нельзя хранить данные доступа к мобильному банку в заметках и SMS-сообщениях, используйте дополнительные способы защиты от несанкционированного доступа – второй PIN-код, код блокировки клавиатуры и меню телефона и пр.

4. Риск перехвата данных в процессе передачи. Банки не остаются в стороне от проблемы. Весьма распространено использование SMS с одноразовыми PIN-кодами для подтверждения каждой операции пользователя. Все банки предоставляют отдельный защищенный канал связи при обращении клиента к мобильным сервисам. Несмотря на все это, универсального оружия против мошеннических схем и хакерских атак пока не придумано [4]. Те же мобильные технологии предполагают SMS-информирование о совершенных операциях. Поэтому, если пользователь видит, что с его счета списаны деньги, которые он не списывал, необходимо как можно быстрее заблокировать карту, чтобы избежать больших потерь.

Важно помнить, что для лучшей сохранности данных нужно регулярно менять пароль. Теоретически возможно, что ваш пароль будет расшифрован, и чем дольше будет установлен один и тот же пароль, тем легче его будет взломать. При смене пароля следует также помнить о требованиях к паролю, которые сделают его более сложным и

безопасным.

ЛИТЕРАТУРА

1. *Овчаров А.П.* Использование модульного подхода в разработке приложений / А.П. Овчаров, В.Р. Лабинцева, А.В. Параскевов // Информационное общество: современное состояние и перспективы развития, сборник материалов XI международного студенческого форума. – Краснодар, Кубанский государственный аграрный университет имени И.Т. Трубилина, 2018. – С. 333-336.

2. *Параскевов А.В.* Перспективы и особенности разработки чат-ботов / А.В. Параскевов, А.А. Каденцева, С.И. Мороз // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ). – Краснодар: КубГАУ, 2017. – № 06(130). С. 395-404. – IDA [article ID]: 1301706030. – URL: http://ej.kubagro.ru/2017/06/pdf/30.pdf.

3. *Параскевов А.В.* IT диверсии в корпоративной сфере / А.В. Параскевов, И.М. Бабенков, О.Б. Шилович // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ). – Краснодар: КубГАУ, 2016. – № 02(116). – С. 1355-1366. – IDA [article ID]: 1161602086. – URL:http://ej.kubagro.ru/2016/02/pdf/86.pdf.

4. *Параскевов А.В.* Критическая информационная инфраструктура в свете концепции информационной безопасности // Итоги научно-исследовательской работы за 2017 год, сборник статей по материалам 73-й научно-практической конференции преподавателей. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2018. – С. 411-412.