УДК 330.1
doi:10.18720/SPBPU/2/id24-186

Сидоров Арсений Леонидович,
аспирант

СЛАБО СТРУКТУРИРОВАННЫЕ ПРОБЛЕМЫ ПРИ РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ЦИФРОВЫХ СЕРВИСАХ И СПОСОБЫ ИХ РЕШЕНИЯ

Россия, Санкт-Петербург, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина),
arseniiy.sidorov@gmail.com

Аннотация. В данной статье рассматривается природа появления оптимизационных слабо структурированных проблем при регистрации пользователей в цифровых сервисах, а также указана конкретная методология по разрешению данных проблем или сведению их к хорошо структурированным проблемам. Также сформулирована и проанализирована центральная проблема оптимизации, которую решает каждый цифровой сервис при регистрации новых пользователей, а также рассмотрены основные верификационные шаги, которые могут быть применены платформой для недопущения регистрации мошенников.

Ключевые слова: цифровые сервисы, верификация, системный анализ, онбординг пользователей, регистрация в цифровых сервисах, мошенничество в цифровых сервисах.

Arsenii L. Sidorov,
Postgraduate (PhD) Student

ILL-STRUCTURED PROBLEMS DURING THE USER ONBOARDING IN DIGITAL SERVICES AND POTENTIAL SOLUTIONS TO THEM

St. Petersburg Electrotechnical University “LETI”, St. Petersburg, Russia,
arseniiy.sidorov@gmail.com

Abstract. This article examines the nature of the emergence of ill-structured optimization problems during users onboarding in digital services, and also indicates a specific methodology for resolving these problems or reducing them to well-structured

problems. The central optimization problem that each digital service solves when registering new users is also formulated and analyzed, and the main verification steps that can be used by the platform to prevent the registration of fraudsters are also considered.

Keywords: digital services, verification, system analysis, user onboarding, registration process in digital services, fraud in digital services.

Введение

В настоящее время человечество живет в эпоху цифровых сервисов. Мы заказываем такси и еду, платим по счетам, находим друзей, инвестируем — с помощью цифровых сервисов. Цифровые сервисы, в свою очередь, в большинстве своем являются частными компаниями и, как любой бизнес, они создаются для извлечения прибыли. С одной стороны, может показаться, что чем больше пользователей цифровой сервис привлечет на свою платформу, тем больше денег удастся заработать. В большинстве случаев такая логика верна, но что, если часть новых пользователей — мошенники, боты или просто клоны другого, уже зарегистрированного пользователя? Засилье мошенников может привести к финансовым или репутационным потерям для компании.

В таком случае, цифровым сервисам нужна определенная модель или сторонний сервис, с помощью которых будет возможно отличить при регистрации настоящего, честного и платящего пользователя от мошенника. При этом, в процессе выявления мошенников образуется целый ряд потенциальных проблем, часть из которых слабо структурированные. В этой статье мы рассмотрим основные из них и предложим теоретические способы их решения.

1. Природа слабо структурированных проблем при регистрации пользователей в цифровых сервисах

Вначале, необходимо дать определение слабо структурированным проблемам. Слабо структурированные проблемы или же смешанные проблемы — это проблемы такого рода, которые содержат в себе как количественные элементы, существенные зависимости которых выяснены хорошо, так и качественные элементы, зависимости которых не определены. При этом качественно выраженные проблемы имеют тенденцию доминировать [1].

Для начала сформулируем центральную проблему оптимизации, которая возникает при регистрации пользователей в цифровых сервисах. Как уже было сказано выше, с одной стороны, чем больше пользователей зарегистрируется на платформе, практически независимо от типа бизнеса, тем больше будет прибыль. Однако число мошенников также вырастет и урон, который они нанесут сложно прогнозировать. [2] Чтобы отсечь мошенников при регистрации в сервисе, необходимо установить набор неких проверок, которые пользователь должен пройти, чтобы получить доступ к платформе.

Самый простой пример — ввести номер телефона и подтвердить доступ к этому номеру телефона введя код из СМС. Однако такую проверку достаточно просто обойти создав виртуальный, одноразовый номер телефона. В таком случае логичным решением может показаться усиление защитных мер и введение дополнительных шагов верификации. В таком случае, стоит учитывать, что чем больше барьеров цифровой сервис устанавливает при регистрации, тем меньшее число пользователей пройдет эту регистрацию. Иными словами, создавая проблемы для мошенников — сервис создает их и для честных пользователей, в конечном счете снижая конверсию в платящего, довольного пользователя.

Таким образом формулируется следующая оптимизационная проблема: цифровому сервису необходимо определить такой набор верификационных шагов, при котором конечная прибыль бизнеса будет наиболее высокой [3]. Уравнение прибыли в данном контексте можно представить следующим образом:

$$\pi = X\,(1 - \delta) * LTV - \sigma - \lambda, \qquad (1)$$

где π — общая прибыль компании, без учета других факторов, не влияющих на процесс онбординга;

X — общее количество пользователей, начавших процесс регистрации;

δ — средний процент пользователей не завершивших процесс регистрации и не ставших клиентами компании;

LTV — средний объем ценности, которую принесет пользователь на протяжении своей «жизни» как клиента;

σ — общий объем потерь цифрового сервиса от мошеннических атак;

λ — общие затраты на проведение верификации пользователей.

Также стоит отметить, что показатели $1 - \delta$ и σ обычно отрицательно коррелирует, то есть чем меньше объем потерь цифрового сервиса от мошеннических атак (чем слабее система верификации), тем больше пользователей успешно завершит процесс регистрации в цифровом сервисе.

На первый взгляд может показаться, что данная проблема, озвученная нами как центральная — может быть явно выражена математически. Однако формула (1) на самом деле достаточно сильно упрощает реальную картину и не учитывает такие факторы как: нормативно-правовые требования, природу бизнеса, конкретные мошеннические схемы, инсайдерскую информацию для мошенников изнутри компании и так далее. Таким образом, мы приходим к выводу, что данная оптимизационная проблема относится к числу слабо структурированных.

Рассмотрим другую, крайне критичную для цифровых сервисов проблему, которую можно отнести к разряду слабо структурированных.

Она посвящена мошенникам и их выявлению по их поведению. С одной стороны, можно построить регрессионную математическую модель, которая бы выявляла мошенников по их поведению и демографическим характеристикам. Однако, как и в предыдущем случае останется значительная часть качественных и не наблюдаемых факторов, которые невозможно или крайне сложно выразить количественно.

Теперь, когда мы рассмотрели проблему посвященную оптимальному набору верификационных шагов и проблему посвященную анализу поведения пользователей при регистрации, можно немного углубиться в детали самих проверок и сформулировать дополнительные, но при этом крайне важные слабо структурированные проблемы.

Один из базовых верификационных шагов, зачастую требуемый к проведению множеством финансовых регуляторов — проверка идентифицирующего документа. Внутри данного процесса также существует различный набор решений, которые может принять цифровой сервис. Так, например, компания может разрешить или запретить загрузку фотографий документа из библиотеки устройства. В случае, если компания запрещает загрузку фото и разрешает только фотографию документа «здесь и сейчас», множество мошеннических схем, использующих заготовленный документ скачанный из сети интернет, не смогут быть применены. С обратной стороны, честные пользователи не всегда имеют идентифицирующий документ при себе, а значит лишаются возможности пройти верификацию в некоторых ситуациях, таким образом, опять же, снижается конверсия в зарегистрированного пользователя. Как следствие, даже сужаясь до рассмотрения одного верификационного шага, все равно возникает слабо структурированная проблема оптимизации, включающая в себя рассмотрение следующих опций: разрешить ли загрузку документа из библиотеки, из каких стран разрешить загрузку документа, какие типы документов разрешить и так далее. В данной проблеме также присутствуют как количественные, так и качественные элементы.

Второй классический этап верификации включает в себя биометрическую проверку. Обычно используется вкупе с документарной проверкой, чтобы удостовериться, что предоставленный документ действительно принадлежит тому, кто сейчас проходит данный процесс верификации и документ не украден. Это проверка происходит путем сравнения фотографии пользователя в документе и фотографии пользователя сделанной с помощью фронтальной камеры в процессе верификации. Однако, перед фирмами здесь также встает слабо структурированная проблема, которую предстоит решить. Сформулировать ее можно следующим образом: Каким именно способом необходимо проводить биометрическую верификацию для отсеивания мошенников, но сохранения максимального количества честных пользователей?

Как и в случае с документарным этапом, здесь существует несколько опций: запросить у пользователя простое селфи или запросить селфи с идентифицирующим документом или запросить прохождение продвинутой проверки “Liveness”. Помимо этого, опять же, можно запретить доступ пользователям из определенного региона или страны, запретить доступ пользователям определенного возраста и так далее.

Как мы видим, все предыдущие проблемы по сути являются оптимизационными задачами, которые необходимо решить, учитывая как количественные, так и качественные элементы.

2. Потенциальные решения слабо структурированных проблем при регистрации пользователей в цифровых сервисах

Кратко рассмотрим потенциальные решения слабо структурированных проблем при регистрации в цифровых сервисах. Каждая из озвученных выше проблем требует разного решения в зависимости от типа бизнеса. Для примера возьмем первую проблему, озвученную ранее как центральную. Для этого рассмотрим основные верификационные шаги и создадим таблицу, показывающую эффект каждого конкретного типового шага на конверсию, защищенность платформы и затраты компании.

Таблица 1

Основные типы проверок и их влияние на конверсию и степень защиты цифровой платформы

Тип проверки	Стоимость для компании	Сложность прохождения проверки для мошенника	Влияние на конверсию
E-mail верификация	1/5	1/5	Слабое негативное
Верификация номера телефона	1/5	1/5	Слабое негативное
Верификация идентифицирующего документа	3/5	3/5	Среднее негативное
Liveness-тест	2/5	4/5	Среднее негативное
AML, PEP, Adverse media проверка	2/5	3/5	Слабое негативное
Проверка адреса	4/5	2/5	Сильное негативное
Проверка происхождения средств	4/5	3/5	Сильное негативное
Валидация номера документа и других данных через локальные базы данных	3/5	5/5	Слабое негативное

Помимо факторов, указанных в таблице 1, цифровым сервисам также стоит учитывать следующие важные аспекты: требования финансового регулятора, общая уязвимость бизнес-модели к мошенническим атакам и располагаемый бюджет.

Для наглядности приведем пример из реального бизнеса. Пользователь, который регистрируется в агрегаторе такси как пассажир вряд ли может по определению серьезно навредить платформе. В таком случае может быть достаточно простого подтверждения номера телефона. С другой стороны, роль водителя гораздо более ответственна, а значит цифровой сервис как минимум должен запросить загрузку водителем своего водительского удостоверения, для проверки на подлинность. Также, полезным шагом будет запросить и биометрическую проверку, чтобы убедиться, что данный пользователь не украл чужое водительское удостоверение.

С другой стороны, при регистрации пользователей в крипто обменнике верификационных шагов будет больше, и сама проверка должна быть строже, так как платформа подразумевает не только ввод средств, но и вывод — а значит может быть использована для отмывания незаконных денежных средств и других махинаций.

Заключение

Таким образом, для решения слабо структурированных проблем, вытекающих из поиска оптимизационного баланса в уравнении с участием потенциальных потерь от мошеннических средств и конверсии в платящего пользователя, решение может быть следующим. Во-первых, необходимо снизить долю качественных элементов, однозначно их определив (например, точно узнать требования регулятора и их соблюдать, если они есть). Во-вторых, нужно определиться, какие верификационные шаги использовать на основе таблицы 1, оценивая потенциальную прибыль компании с помощью формулы (1). В-третьих, компании должны постоянно проверять собственную цифровую платформу на уязвимости, находить их и оперативно устранять, иначе — их найдут мошенники.

Список литературы

1. Системный анализ и принятие решений: Словарь-справочник / Под ред. В.Н. Волковой, В.Н. Козлова. – М.: Высшая школа, 2004. – 616 с.

2. Zalando defrauded of 18.5 million euros [Electronic Source]. – September 16, 2015. – URL: https://ecommercenews.eu/zalando-defrauded-of-18-5-million-euros/ (date of access: 10.10.2023).

3. Сидоров А.Л. Актуальность внедрения дополнительных защитных мер для цифровых сервисов при регистрации пользователей // Актуальные аспекты модернизации российской экономики: материалы IX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых / Под общ. ред. д-ра техн. наук, проф. И.А. Брусаковой. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2022. – С. 282–287.

4. Chakraborty S., Das D. An overview of face liveness detection // International Journal on Information Theory. – 2014. – Vol. 3 (2). – DOI: 10.5121/ijit.2014.3202.