

Из графика и по значениям в таблице 1 видно, что **максимальная прибыль достигается** при значении $n = 6$ и равна 11421 484 рублей в месяц.

Вывод:

При прочих постоянных параметрах, выгоднее всего нанять 18 инспекторов (по 6 инспекторов одновременно). Тогда прибыль будет оптимальной и равна 11421484 рублей в месяц.

Повышение эффективности труда является важной задачей в любой общественно – экономической формации. Основными факторами, влияющими

на повышение производительности труда, являются повышение технологического уровня, совершенствование управления на производстве, различные отраслевые факторы.

Список литературы

1. Шевченко Д.В. Основные параметры систем массового обслуживания. – М. ЮНИТИ, 2012. – 207с.
2. Волошин Г.Я. Методы оптимизации в экономике: Уч. пособие. – М.: ДИС, 2004. – 320 с.

ВНЕДРЕНИЕ ТЕХНОЛОГИИ OPEN API В БАНКОВСКОЙ СФЕРЕ



Пузанков Артем Михайлович

Студент 3 курса, факультет информационных технологий Московского политехнического университета



Чикунев Иван Михайлович

кандидат технических наук, заведующий кафедры «Инфокогнитивные технологии» Московского политехнического университета.

Аннотация: В статье рассмотрены новые внедрения в банковскую сферу технологий Open Banking, которые используют средства OpenApi. Общедоступный набор программных инструментов Open Api позволяющий наладить взаимодействие между приложениями.

Ключевые слова: Open Api, банковская сфера, уязвимости, безопасность.

Abstract: The article discusses the new implementation of Open Banking technologies in the banking sector, which use OpenApi tools. Public set of software tools Open Api allows you to establish interaction between applications.

Keywords: Open Api, banking, vulnerabilities, security.

Под современной автоматизированной банковской системой в настоящее время понимается интегрированная система с единым информационным пространством, эффективное использование которой требует изменения сложившейся технологии работы банка.

Для любой банковской организации получение прибыли – основная цель существования, отчего рассмотрим его в качестве платформы, задача которой коммуникация людей, имеющих деньги, с людьми, нуждающимися в них. Сейчас подобными задачами занимаются технологические компании (Apple, Spotify, Uber и др.). Происходит это потому, что они смотрят не «только в себя», но и ориентируются на передовые технологии в IT сфере. [2]

Новым внедрением в банковскую сферу стала технология Open Banking, использующая средства Open Api. Open Api – общедоступный набор программных инструментов, который позволяет наладить взаимодействие между приложениями.

Причиной развития данной технологии в банковской сфере является появление большого количества стартапов, которые предлагают новые способы повышения объёмов продаж, оптимизации работы с клиентской базой и привлечение новых клиентов для банка. Возникновение большого числа инновационных продуктов и сервисов на рынке банковских услуг неминуемо, чем облегчится доступ конечного потребителю к этим услугам и повысится комфортность их использования. [1]

Все банковские данные делятся на три типа:

- Закрытые данные, или внутренние регламенты, правила и алгоритмы, которые используются внутри организации, данные о рентабельности, (т.е. информация, носящая характер коммерческой и банковской тайны).
- Разделяемые данные. Все данные, которые касаются клиентов, транзакций, счетов и баланса карт клиентов.
- Открытые данные. Прочая общедоступная информация (типы вкладов, отделения, кредитная ставка и т.д.)

Когда речь идет об открытом API банка, подразумевается использование разделяемых и открытых данных. При этом и сами сервисы API делятся на два типа:

- С авторизацией при обращении
- Без авторизации

Авторизация необходима для получения разделяемых данных, для получения открытых данных авторизация не требуется.

Число различных ресурсов и операций, которые банки могут предоставлять через OpenAPI, измеряется несколькими сотнями, потому помимо технической платформы, (такой как Swagger или других аналогичных решений), удобство API достигается также за счет правильно структурированного набора сервисов. Основной спектр бизнес-операций, предлагаемых приложениями мобильного банкинга для физических лиц от передовых российских компаний – разработчиков систем дистанционного банковского обслуживания, можно разделить на несколько групп по назначению функций:

- сервисы авторизации и безопасности (аутентификация в системе, получение паролей 3-D Secure, привязка мобильного устройства к учетной записи клиента и др.);
- информационные сервисы (получение списка счетов/карт/кредитов клиента, формирование выписок, публикация списка отделений и банкоматов и др.);
- платёжные сервисы (перевод между счетами клиента, оплата услуг, переводы по номеру карты и др.);
- сервисы подачи заявок (на открытие или закрытие вклада, получение кредита и др.).

Без правильной реализации, с точки зрения информационной безопасности, даже очень хорошо спроектированный API не будет актуален. Чтобы сторонние разработчики с помощью средств API смогли воплотить свои идеи в реальный продукт, а после, специалисты по информационной безопасности смогли бы провести анализ рисков, возникающих при эксплуатации данного ПО, банку необходимо создать тестовую систему – эмулятор, где программисты смогут протестировать функциональные характеристики API. Подобные «песочницы» могут быть организованы совместно с демо-стендами интернет-банков. Разработчики, имея доступ к демо-версии интернет-банка, смогут изменить их возможности, предоставляемые клиентам банка, предложить свой вариант реализации, заложенного функционала или создать набор дополнительных опций, отсутствующих в текущей системе дистанционного банковского обслуживания. [3]

В любом банке к обеспечению безопасности относятся очень щепетильно. Особенно когда речь заходит о безопасности их компьютерных систем, необходимых для работы современного банка. Сформировалась тенденция, открывать свободный доступ любому желающему к тому, что десятилетиями принято было тщательно оберегать от проникновения посторонних.

Для большинства банков проще отбросить эту идею, чем подумать о том, как технически организовать безопасный доступ по открытому API к своему IT-ядру. Кроме того, некоторые банки могут рассматривать открытие своих API, как создание собственными руками благоприятной среды для возникновения потенциальных конкурентов.

Рассмотрим ситуацию с другой стороны и попытаемся ответить на вопросы:

- Какие угрозы несет в себе OpenAPI для банковской организации?
- Как обеспечить безопасность?

В первую очередь нужно сказать о некачественных приложениях, разработанных технической компанией, которые решили воспользоваться Open API банка. Из-за плохо спроектированной структуры ПО? Из-за неправильной реализации защиты данных и каналов связи банк может понести большие потери: потерять персональные данные, данные несущие

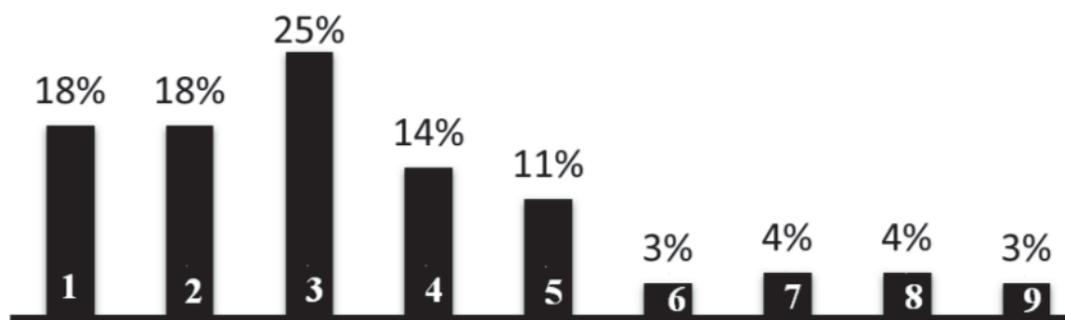


Рисунок 1. Нарушения установки мер информационной безопасности в дистанционном банковском обслуживании.

коммерческую и банковскую тайну, утратить доступ к счетам и вкладам клиентов. [4]

В 44% дистанционного банковского обслуживания обнаружены уязвимости, которые имеют высокий уровень риска. Большая часть из них заключается в ошибках реализации механизмов защиты, в эти механизмы входят механизм идентификации, аутентификации и авторизации. На втором месте стоят уязвимости в коде приложений, на третьем – конфигурационные ошибки.

На рисунке 1 приведена диаграмма известных исходов после нарушения установки мер информационной безопасности в дистанционном банковском обслуживании и их процентная составляющая:

1. Кража денежных средств со стороны авторизованного пользователя (18 %)
2. Доступ к СУБД или файловой системе, НДС к банковской тайне (18%)
3. НДС к сведениям, составляющим банковскую тайну на уровне отдельных клиентов (25 %)
4. Кража денежных средств со стороны внешнего злоумышленника, доступ к ОС или СУБД (14 %)
5. Кража денежных средств авторизованного пользователя, доступ к СУБД или файловой системе (11 %)
6. Кража денежных средств со стороны внешнего злоумышленника путем установки вредоносного ПО на мобильное устройство (3 %)
7. Возможный фишинг, реализованный за счет небезопасной передачи данных в мобильном приложении (4 %)
8. Отказ в обслуживании клиентской части мобильной системы ДБО (4 %)
9. Отказ в обслуживании пользовательской системы ДБО (3 %)

В 2016 году компанией Positive Technologies был проведен анализ защищенности дистанционного банковского обслуживания ряда крупнейших банков России. Было рассмотрено 28 систем дистанционного банковского обслуживания. Две трети систем являлись собственными разработками (были использованы языки Java, C# и PHP), оставшиеся были раз-

вернуты на базе платформ известных вендоров. При этом большая часть систем дистанционного банковского обслуживания (74 %) находилась в промышленной эксплуатации, другие же уже находились на этапе тестирования.

В настоящее время происходит качественное изменение в подходе банков к автоматизации. Появление на финансовом рынке новых технологий и инструментов, переход зарубежных банков от технологии централизованного учета и терминальной обработке данных к технологии клиент-сервер и распределенной обработке привели к пересмотру концепции автоматизации и ее роли в стратегии и тактике банковской деятельности. Для поддержания общей конкурентоспособности в банках разрабатывают новые модели анализа факторов риска, уровня инвестиционной привлекательности проектов. Содержание банковских технологий рассматривают как совокупность действий, обеспечивающих организацию сервисного обслуживания, соответствующего запросам клиента, поддержание конкурентоспособности заведения.

Список литературы

1. Булатова А. И. Банковская система России: новые технологии в повышении эффективности развития // Инновационная экономика: материалы II Междунар. науч. конф. (г. Казань, октябрь 2015 г.). – Казань: Бук, 2015. – С. 39
2. Илкин Н. С. Инновации в деятельности коммерческих банков // «Концепт», Т.4/2017 г., с. 142
3. Оголиха С. Д. Оценка необходимости применения инноваций в банковской системе России // Скиф. Вопросы студенческой науки. Экономика и экономические науки, №14/2017 г., с. 60
4. Назаренко Г. В. Банковские инновации как результат инновационной банковской деятельности в условиях конкурентной борьбы // Финансовые исследования. Экономика и экономические науки, №2/2014 г., с. 67
5. Официальный сайт аналитического центра Национального агентства финансовых исследований «НАФИ» [Электронный ресурс]. Режим доступа: <https://nafir.ru/>