анализа. Это представляется возможным достигнуть за счет сокращения сроков его проведения, возможностей использования большого количества информации о финансово-хозяйственной деятельности, сокращения ошибок при расчетах, использования методов моделирования и оптимизации, которые будут намного дольше выполняться вручную и традиционными методами.

Список цитируемых источников

1. *Тонких, Д. О.* К вопросу об эффективности финансового менеджмента в организации / Д. О. Тонких // Концепт. — 2017. — Т. 4. — С. 413—418.

УДК 004.42

А. С. Батайкин, И. А. Камленок
Учреждение образования «Барановичский государственный университет», Барановичи

РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ ОБРАБОТКИ SIP-ЗВОНКОВ, С ОБРАБОТКОЙ НОМЕРОВ, СТАТИСТИКОЙ ЗВОНКОВ И ГРАФИЧЕСКИМ ИНТЕРФЕЙСОМ

Введение. На сегодня большинство компаний использует ИТ в управлении своим бизнесом. Информационные технологии позволяют делать бизнес более наглядным, более управляемым, более прогнозируемым.

Основная часть. Разработка системы обработки SIP-звонков позволяет в автоматическом режиме проводить обработку входящих/исходящих звонков со сбором статистики о проходящих звонках, что даст возможность оператору отслеживать наиболее нагруженное время, в которое делается наибольшее количество звонков, и своевременно принять меры по предоставлению наилучшего качества связи своим пользователям.

Поставленная задача предполагает разработку базы данных, серверной части и интерфейса к ней.

Серверная часть реализована при помощи технологии Java EE с использованием различных фреймворков на языке Java.

Для хранения структуры данных используется СУБД MySQL 8.0.15, так как это одно из наиболее совместимых решений совместно с технологиями сервера, официально поддерживаемыми Oracle.

Для реализации интерфейса были использованы следующие технологии:

- HTML5 — стандартизированный язык разметки веб-документов [5];
- CSS3 — каскадная таблица стилей, формальный язык описания внешнего вида веб-документов [4];
- Matrial.UI — JavaScript-библиотека, которая содержит набор высококачественных компонентов для стилизации приложения [3];
- React — JavaScript-библиотека для разработки пользовательских интерфейсов [1];
- Redax — шаблон для JavaScript, предназначенный для управления состоянием приложения [2].

В приложении используется база данных, содержащая следующие таблицы:

– “Users” — содержит всю необходимую информацию о пользователе (номер телефона, Ф. И. О. пользователя, роль пользователя в системе, используемый пользователем тариф);

– “Blacklist” — содержит информацию о черном списке пользователя (id чёрного списка, номер телефона владельца);

– “Blacklist_user” — реализует связь многие-ко-многим для таблиц “Blacklist” и “Users”;

– “Hibernate_sequence” — принадлежит технологии работы с сущностями базы данных “Entity”, содержит информацию о следующем значении автоматически генерируемого поля;

– “Authorization” — содержит информацию об авторизированных пользователях в системе (id авторизации, пароль пользователя, номер телефона пользователя);

– “Tariffs” — содержит информацию о всех доступных тарифах в системе (название тарифа, стоимость одного звонка);

– “Configurations” — содержит информацию о конфигурировании всей системы (название конфигурации, описание);

– “Statistics” — содержит информацию о статистике звонков, проходящих через систему (название статистики, описание).

Физическая модель базы данных представлена на рисунке 1.

База данных состоит из восемь таблиц, связи между которыми обеспечивают наименьшую избыточность данных.

При успешном запуске приложения обработки Sip-звонков и переходе в браузере по адресу сервера открывается страница с авторизацией, которая представлена на рисунке 2.

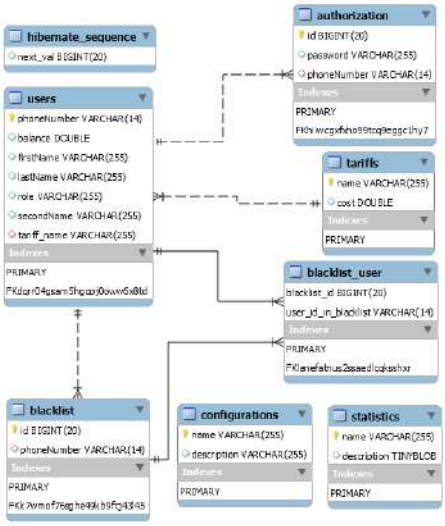

Рисунок 1 — Физическая модель базы данных

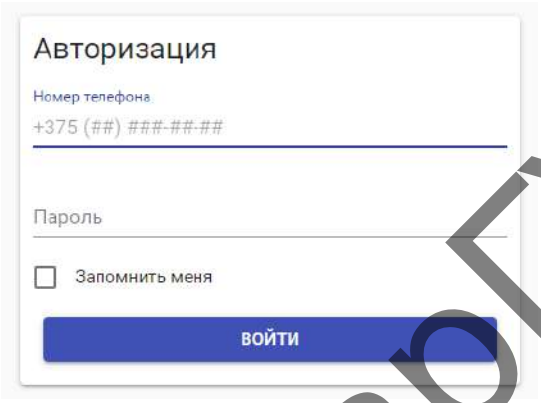

Рисунок 2 — Страница авторизации

Для авторизации пользователя необходимо ввести номер телефона и пароль, а ткаже можно выбрать пункт «Запомнить меня», если не хотим проходить процесс авторизации еще раз при случайном закрытии страницы сайта.

Так как основная задача сервиса — это принимать, обрабатывать и перенаправлять звонки, то показать принцип работы и более полный функционал возможно посредством специального программного обеспечения “SIPP”. По своему внутреннему таймеру сервер обновляет статистику звонков, которую можно просмотреть в панели администратора (рисунок 3).

Сервис обладает функционалом по автоматическому преобразованию номера в международный формат. Если пользователь набирает номер, указанный не в международном формате (например, семь цифр без кода) либо номер, начинающийся с «80», то специально созданный модуль по обработке трафика конвертирует номер в международный формат и соединят абонентов (рисунок 4).

Данный программный продукт позволит принимать, обрабатывать, перенаправлять SIP-звонки, а также регистрировать новых пользователей сети, просматривать статистику звонков.

Заключение. Создаваемый программный продукт позволит в реальном времени следить за статистикой телефонного сервиса, а также пользователям контролировать свой аккаунт, что повысит клиентоориентированность и прибыль предприятия.

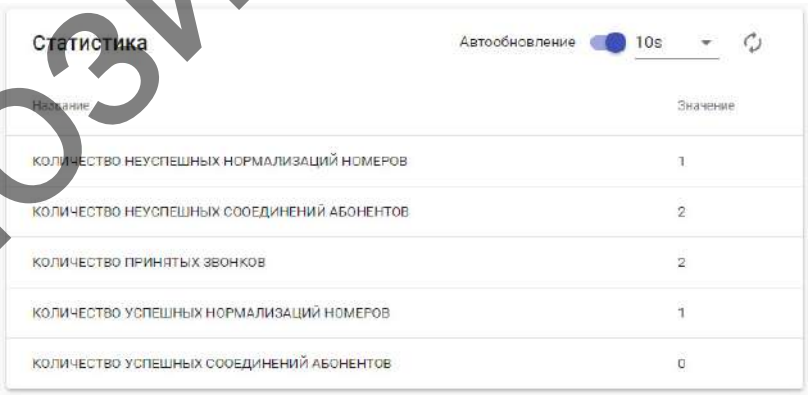

Рисунок 3 — Обновленная статистика

```
Message: Entering 'PhoneChecker' normalizeNumber << |#]
Message: Entering 'PhoneChecker' normalizeNumber phoneNumber = 1111111 |#]
Message: Entering 'PhoneChecker' normalizeNumber phoneNumber = +375291111111 >> |#]
```

Рисунок 4 — Лог нормализации номера

Список цитируемых источников

1. Документация React [Электронный ресурс]. — Режим доступа: http://reactjs.org/ . — Дата доступа: 16.04.2019.
2. Документация Redax [Электронный ресурс]. — Режим доступа: http://npmjs.com/package/redax . — Дата доступа: 16.04.2019.
3. Документация Material-UI [Электронный ресурс]. — Режим доступа: http://material-ui.com/ . — Дата доступа: 17.04.2019.
4. *Макфарланд, Д. С.* Новая большая книга CSS / Д. С. Макфарланд. — СПб. : Питер, 2017. — 720 с.
5. *Фримен, Э.* Изучаем HTML, XHTML и CSS / Э. Фримен — СПб. : Питер, 2010. — 656 с.

УДК 004.056.53

В. О. Богушевич, Е. Н. Босая
Учреждение образования «Барановичский государственный университет», Барановичи

ЗАЩИТА ИНФОРМАЦИИ В СЕТИ

Введение. Информационная безопасность в Сети — действия, направленные на защиту работоспособности и целостности сети и данных, для предотвращения и мониторинга попыток несанкционированного доступа, модификации информации, возможного отказа работы всей компьютерной сети и других сетевых ресурсов.

Современный мир — это мир компьютерной техники, и люди, живущие в этом мире, чувствуют себя в нём комфортно, они легко осваивают компьютер, мобильные устройства, новомодные гаджеты и ими пользуются. Интернет сегодня — это гораздо больше, чем просто общение с друзьями, социальные сети, игры, онлайн-покупки [1, с. 367]. Это открытая система информации, и, если кажется, что вам нечего скрывать или ваша информация никому не нужна, вы глубоко заблуждаетесь. Любая информация о вас может быть использована не теми, кому она предназначалась. Абсолютно любая информация, которой ежедневно делятся люди с друзьями и близкими, может в любой момент оказаться у злоумышленников.

Основная часть. Быстрое развитие процессов автоматизации и проникновение вычислительных машин во все сферы жизни привели к появлению очень важной проблемы надежного обеспечения сохранности информации. Особую роль в этом процессе сыграло появление персональных ЭВМ, локальных и глобальных сетей, спутниковых каналов связи, эффективной технической разведки и конфиденциальной информации, программное обеспечение и другие информационные технологии, доступные для широкой публики. Широкое распространение ПК и невозможность эффективного контроля за их использованием привели к снижению уровня безопасности информационных систем, что существенно обострило проблему защиты информации [2, с. 392].

Информационная безопасность — состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Информационная безопасность включает в себя такие аспекты: целостность информации — предотвращение несанкционированной модификации или разрушения информации; конфиденциальность — предотвращение несанкционированного ознакомления с информацией.

Многие организации не до конца понимают истинную силу виртуальной интернет-угрозы, поэтому ограничиваются лишь элементарными средствами защиты. Как правило, это традиционная блокировка компьютерного вируса или введение ограничений на спам-сообщения в электронной почте [3, с. 594].

В сложившейся ситуации обработка данных вывела проблемы информационной безопасности в ранг самых важных государственных проблем. Решение проблемы плохой информационной безопасности предполагает комплекс мер, прежде всего такие действия государства, как разработка системы классификации, документирование методов защиты информации, правил доступа к данным и меры наказания против нарушителей информационной безопасности. Порядок хранения данных должен быть четко определен в правовых актах и предусматривать полную безопасность носителей, контроль за работой с информацией, ответственность за несанкционированный доступ к носителям в целях их копирования, изменения или уничтожения.

Обеспечение информационной безопасности в компьютерных сетях и ПК, работающих автономно, достигается комплексными организационными, техническими и программными мерами.

Организационные методы защиты информации включают в себя: доступ к обработке и передаче конфиденциальной информации только определенным должностным лицам; исключение посторонних лиц для просмотра содержания материалов, обрабатываемых через дисплей, принтер.

Технические методы: ограничение доступа в помещения, в которых происходит обработка информации (сигнализация и устройства, ограничивающие доступ в помещения, и установка на дверях помещений кодовых замков); хранение носителей информации и документов в закрытых от несанкционированного доступа сейфов и помещениях; уничтожение информации на жестких дисках при отправке ком-