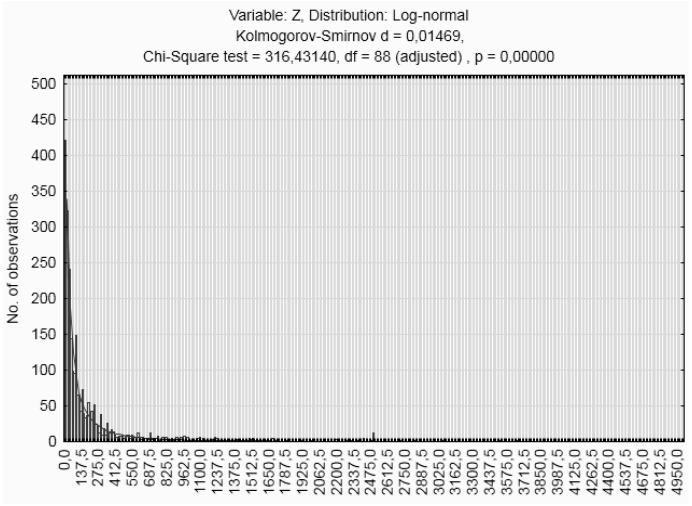

Рисунок 5 — Распределение габаритного размера по оси Z

Как видно из рисунков 3—5, полученные результаты похожи на ожидаемое log-нормальное распределение, если учитывать определённую погрешность, вызванную, по всей видимости, недостаточным количеством обработанных деталей. Значения критерия Колмогорова-Смирнова показывают на хорошее соответствие закону логарифмически нормального распределения.

Заключение. Хочется отметить, что в работе был произведён сбор и анализ информации о габаритных размерах деталей и сборочных единиц; была написана универсальная программа, производящая импорт данных о деталях, и затем — экспорт статистических данных о материале и габаритах модели; получены габаритные размеры свыше двух с половиной тысяч деталей, которые были проанализированы и показаны в виде гистограмм.

В результате получена зависимость, максимально приближенная к логарифмически нормальному виду.

Список цитируемых источников

1. *Нестеров, Д. К.* Экономия металла при производстве и применении сортового проката / Д. К. Нестеров. — М. : Металлургия, 1990. — 192 с.

2. *Норсеев, С. А.* Разработка приложений под КОМПАС в Delphi / С. А. Норсеев. — Б. м. : [б. и.], 2013. — 346 с.

Материал поступил в редакцию 25.02.2015 г.

УДК 004.658.2

Д. А. Викторович, А. В. Гаврон, А. В. Шах
Учреждение образования «Барановичский государственный университет», Барановичи

ЗАЩИТА ИНФОРМАЦИИ В БАЗАХ ДАННЫХ

Введение. Развитие новых информационных технологий приводит к тому, что информационная безопасность становится обязательной. Существует огромное количество систем, в которых безопасность данных играет первостепенную роль. Под безопасностью системы подразумевается её защищённость от случайного или преднамеренного вмешательства в нормальный процесс функционирования, попыток хищения данных и их несанкционированному редактированию [1].

Цель работы заключается в защите пользовательских данных от хищения и случайного редактирования.

Основная часть. При работе над проектом основная задача заключалась в разработке системы защиты информации, хранящейся в базе данных. Для работы с базой данных была использована СУБД MySQL. В качестве предметной области была использована банковская сфера деятельности.

В данной программе использовалось несколько способов защиты информации:

1. Парольный доступ к серверу БД. Для того чтобы подключиться к серверу базы данных необходимо знать верные логин и пароль, в противном случае подключиться просто не выйдет (рисунок 1).

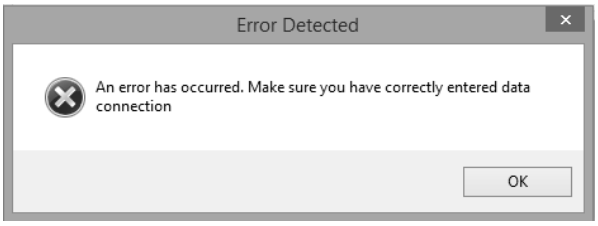

Рисунок 1 — Пример парольной защиты доступа к серверу

2. Разграничение прав доступа. Приложение адаптировано к разграничению прав доступа, администратор сервера через систему администрирования сервером (в нашем случае MySQLWorkbrench) может распределить права доступа пользователей (сотрудников) к базе данных тем самым предотвратив утечку важных данных. Попытка вывести запрещённые к просмотру данные вызовет прерывание выполнения операции и сгенерирует сообщение с предупреждением о запрете доступа (рисунок 2).

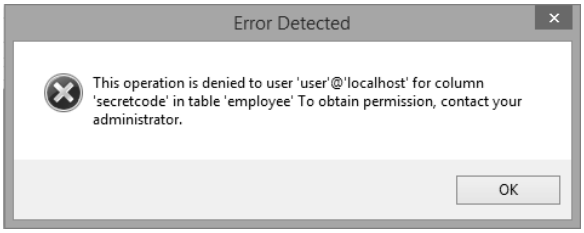

Рисунок 2 — Пример ошибки сообщающей о недостатке прав для выполнения операции

3. Защита ответственности других пользователей (сотрудников).Так как приложение разрабатывается для банковской сферы, необходимо предотвратить возможность махинаций среди персонала. Поэтому в программу был добавлен секретный пароль сотрудника «secretcode», который необходимо вводить при добавлении нового контракта для аутентификации сотрудника. В случае неверного ввода данного пароля контракт не будет создан и будет сгенерировано сообщение об ошибке (рисунок 3).

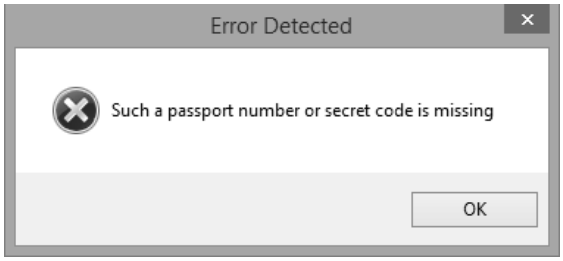

Рисунок 3 — Ошибка, генерируемая при неверном вводе секретного кода сотрудника

4. Защита от ошибок, вызванных человеческим фактором. Информация тщательно защищена от ошибок, вызванных человеческим фактором. В случае попытки заполнения полей данными противоречащими другим таблицам, либо попытки добавления записи со значением, содержащим нулевое поле, а также попытка заполнения данными несоответствующего типа будет генерироваться ошибка о том, что поле не может быть нулевым, либо не подходит по типу (рисунки 4; 5).

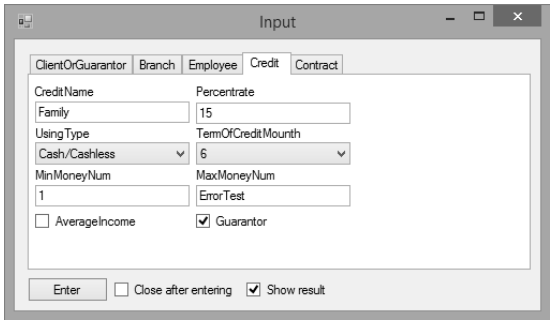

Рисунок 4 — Ввод данных

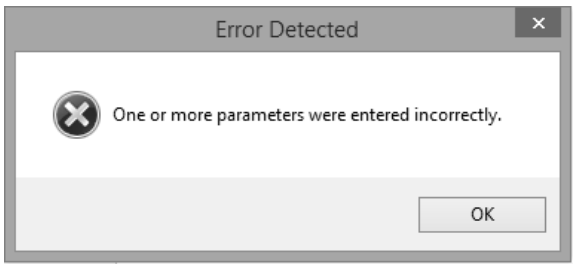

Рисунок 5 — Ошибка, генерируемая при вводе значения неверного типа

5. Защита шифрованием особо важных полей. Поле «secretcode» находится в базе данных в зашифрованном виде и переведён в бинарный формат (рисунок 6) на случай утечки информации и может быть расшифровано только известным ключом. Шифрование полей происходит стандартными функциями SQL с использованием ключа.

Для шифрования были использованы стандартные функции СУБД MySQL: Encode(), Decode().

DECODE(str, key_str). Считывая зашифрованную строку str, созданную ранее посредством функции ENCODE(), расшифровывает её с помощью строки пароля key_str и возвращает результат расшифровки. Возвращает результирующую строку или NULL, если str имеет значение NULL

	employeeid	fioemployee	birthdate	recruited	passportnumber	passportissueddate	passportissuedwho	phone	branch_branchid	secretcode
	3	Angelina Vasil...	1985-07-04	2011-03-03	96584017201	2014-10-30	Baranovichskiy GOVD	+375 (0...	1	BLOB
	4	Vadim Karaim	2014-12-02	2014-12-02	11112222111	2014-12-02	Minskoe GOVD	+375 (0...	2	BLOB
	9	Steve Jobs	1955-06-16	2014-12-11	984256ASD16	2014-02-13	Grodno GOVD	+375 (0...	3	BLOB
	10	Bill Gates	2014-12-11	2014-12-11	0002220021A	2014-12-11	Los Angeles	+375 (0...	1	BLOB
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Рисунок 6 — Зашифрованное секретное поле secretcode

6. Экранирование символов входных данных. Во избежание ввода в поле вредоносного запроса злоумышленником часть символов запрещена к использованию. Например, такие символы как точка с запятой.

Заключение. В данной работе было разработано защищённое приложение для работы с базами данных. Были использованы: парольный доступ к серверу базы данных, разграничение прав доступа, дополнительная идентификация пользователей (при некоторых операциях), защита от ошибок, вызванных человеческим фактором, шифрование данных, экранирование символов входных данных.

Список цитируемых источников

1. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] / Совет Безопасности Российской Федерации. — Режим доступа: http://www.scrf.gov.ru/documents/5.html. — Дата доступа: 10.02.2015.

2. *Титоренко, Г. А.* Информационные технологии управления / Г. А. Титоренко. — 2-е изд. — М. : Юнити-Дана, 2003. — 439 с.

Материал поступил в редакцию 24.02.2015 г.

УДК 004.94

С. Л. Гусева, И. А. Страхов, А. Н. Ивутин

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тульский государственный университет», Тула, Российская Федерация

ПРИМЕНЕНИЕ АППАРАТА ПОЛУМАРКОВСКИХ СЕТЕЙ В ЗАДАЧАХ ОЦЕНИВАНИЯ ВРЕМЕНИ ВЫПОЛНЕНИЯ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ

Введение. Исследование характеристик протекания информационных процессов является одним из важнейших вопросов современных исследований в области проектирования компьютерных систем разной степени сложности. Информационная система, при проектировании которой сбалансированы все основные показатели, должна не только выполнять свои непосредственные функции, но и оптимально использовать выделяемые ресурсы, особенно условия ограничения по вычислительной или временной сложности.