МРНТИ 81.93.29 https://doi.org/10.26577/JMMCS-2019-4-m10

**[1]О.А. Усатова, [2]С.Е. Нысанбаева, [3]В. Вуйцик**

[1]докторант PhD, Казахский национальный университет имени аль-Фараби,
г. Алматы, Казахстан, E-mail: olgaussatova@gmail.com
[2]д.т.н., ассоциированный профессор,
Институт информационных и вычислительных технологий, г. Алматы, Казахстан,
E-mail: sultasha1@mail.ru
[3]д.т.н., профессор, Люблинский технологический университет, г. Люблин, Польша,
E-mail: waldemar.wojcik@pollub.pl

# ИССЛЕДОВАНИЕ И РАЗРАБОТКА МОДЕЛИ ЗАЩИТЫ БАЗЫ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ

**Аннотация**. В статье описаны методы защиты базы данных и информации, хранящейся в ней. Проведен анализ кибератак на информационные системы. Рассмотрены некоторые компании, которые предоставляют услуги по защите информации хранящейся в базах данных, а также структурированных и неструктурированных данных. Описана разработанная модель защиты базы данных, которая отображает последовательность метод шифрования и дешифрования. Разработан алгоритм методов шифрования / дешифрования информации, который основан на использовании криптографического метода шифрования Base64. Описан фиксированный префикс. Представлен результат перекодировки Base64 для каждого ASCII-читаемого символа и цифры. Кратко описана инфляция префикса. Осуществлена программная реализации описанного алгоритма, разработанная под операционную систему Windows в среде разработки Embarcadero RAD Studio на языке программирования Deplhi с применением интеграции с другими языками программирования и подключенных системных библиотек. Дано подробное описание инструкции пользователя рассматриваемого алгоритма. Проведен анализ программной реализации предложенного алгоритма.

**Ключевые слова**: защита базы данных, защита информации, безопасность данных, модель защиты, приложение, база данных, шифрование, дешифрование.

[1]О.А. Усатова, , [2]С.Е. Нысанбаева, [3]В. Вуйцик
[1]докторант, әл-Фараби атындағы қазақұлттық университеті,Алматы қ., Қазақстан,
E-mail: olgaussatova@gmail.com
[2]т.ғ.д., қауымдастырылған профессор, Ақпараттық және есептеу іштехнологиялар институты,
Алматы қ., Қазақстан, E-mail: sultasha1@mail.ru
[3]т.ғ.д., профессор, Люблин қ. техникалық университеті, Люблин, Польша,
waldemar.wojcik@pollub.pl

**Дерекқор қорғанысы ақпараттық жүйесін зерттеу және моделін құру**

**Аңдатпа**. Мақалада деректер базасын және ақпарат қорғаудың тәсілдері сипатталған. Ақпараттық жүйелердегі кибершабуылдарға талдау. Деректер базасында сақталатын ақпаратты, сондайақ құрылымдалған және қҰрылымданбаған деректерді қорғау қызметтерін ұсынатын кейбір компаниялар қарастырылады. Дерекқорды қорғаудың дамыған моделі сипатталған, онда шифрлау және дешифрлау әдісінің реттілігі көрсетілген. Base64 криптографиялық шифрлау әдісін қолдануға негізделген ақпаратты шифрлау / дешифрлау әдістерінің алгоритмі жасалды. Бекітілген префикс сипатталған. Әр ASCII оқылатын таңба мен сан үшін Base64 кодтау нәтижесі ұсынылған. Қысқа сипатталған инфляция префиксі. Deplhi бағдарламалау тілінде Embarcadero RAD Studio дамыту ортасында Windows басқа операциялық жүйелері үшін әзірленген, басқа бағдарламалау тілдерімен және жүйелік кітапханалармен интеграцияны қолдана отырып, сипатталған

алгоритмнің бағдарламалық қамтамасыздандыруы іске асырылған. Пайдаланушыға алгоритм бойынша нұсқаулықтардың толық сипаттамасы келтірілген. Ұсынылған алгоритмнің бағдарламалық қамтамасыз етілуіне талдау жасалған.
**Түйін сөздер**:дерекқорды қорғау, ақпаратты қорғау, деректер қауіпсіздігі, қорғау моделі, қосымша, дерекқор, шифрлау, дешифрлау.

[1]O.A.Ussatova, [2]S.E. Nyssanbayeva, [3]W. Wojcik
[1]doctoral student, al-Farabi Kazakh National University, Almaty, Kazakhstan,
E-mail: olgaussatova@gmail.com
[2]Doctor of Engineering, associate professor, Institute of Information and Computational Technologies,
Almaty, Kazakhstan, E-mail: sultasha1@mail.ru
[3]Doctor of Engineering, professor, Lublin University of Technology, Lublin, Poland,
E-mail: waldemar.wojcik@pollub.pl

**Research and development of an information system database security model**

**Abstract**. The article describes the methods of protecting the database and the information stored in it. The analysis of cyberattacks on information systems is presented. Some companies that provide services to protect information stored in databases, as well as structured and unstructured data, are considered. The developed database protection model is described, which displays the sequence of the encryption and decryption method. An algorithm of information encryption / decryption methods has been developed, which is based on the use of Base64 cryptographic encryption method. A fixed prefix is described. The Base64 transcoding result for each ASCII-readable character and digit is presented. Briefly described inflation prefix. A software implementation of the described algorithm was implemented, developed for the Windows operating system in the Embarcadero RAD Studio development environment in the Deplhi programming language, using integration with other programming languages and connected system libraries. A detailed description of the user instructions for the algorithm in question is given. The analysis of the software implementation of the proposed algorithm is carried out.

**Key words**:protection of the database, information security, data security, protection model, application, database, enciphering, decoding.

## 1 Введение

На современной стадии эволюции нашего общества некоторые традиционные ресурсы человеческого развития понемногу утрачивают свое первоначальное предназначение. На смену им приходит новые информационные ресурсы, единственные продукты не убывающие, а растущие со временем. Информация стала в настоящее время одним из основных ресурсов научно-технического и социально-экономического прогресса в мировом сообществе [1]. Информация имеет определенную стоимость, следовательно, сами факты получения данных злоумышленниками приносят им определенные доходы, ослабив тем самым возможность конкурента к равному коммерческому состязательству. Главной целью злоумышленников является получение сведений о составе, состояниях и видах деятельности объектов, являющихся конфиденциальными интересами в целях насыщения своей информационной потребности. Корыстные цели злоумышленников или конкурентов могут заключаться и во внесении определенного изменения в состав данных, которые циркулируют на объектах конфиденциального интереса. Такие действия могут приводить к дезинформации в определенной сфере деятельности с данными, и результатах решения некоторой задачи. Более опасным является уничтожение накопленного информационного массива в документной или компьютерной формах или программного продукта. В связи с этими фактами большое

значение приобретают методы организации и создание эффективных систем информационной безопасности [2]. Информационной безопасностью называется комплекс мер по защите данных от неавторизованного доступа, разрушений, модификаций, раскрытий или задержки при доступе. В информационную безопасность включаются меры по защите процесса создания информации, её ввода, обработки и вывода. Цель информационной безопасности состоит в том, чтобы обезопасить ценность систем, защищать и гарантировать точность и целостность данных, а также минимизировать последствия, которые могут возникнуть в том случае, когда данные будут модифицированы или разрушены. В рамках информационной безопасности требуется учет всех действий, в ходе которых информация создается, подвергается модификации, когда к ней осуществляется доступ или она распространяется по сети [3]. Целью исследования являются средства защиты баз данных для обеспечения безопасности, целостности и конфиденциальности информации. Для решения поставленной цели рассматривались задачи, направленные на исследования атак и средств защиты баз данных. Построена и программно реализована модель защиты баз данных.

## 2 Обзор литературы

База данных на сегодняшний день является незаменимым инструментом для хранения и обработки информации. Любая компания, хранящая и обрабатывающая информацию в базах данных (БД), может столкнуться с хищением конфиденциальных сведений. Для проведения атак на информационные системы злоумышленники используют широкий спектр «технологий» — DDoS атаки, получение несанкционированного доступа путем компрометации учетных записей пользователей, вредоносное программное обеспечение различных типов, взлом службы доменных имен и приложений. Значительную долю успешных внешних атак на информационные системы были проведены при помощи SQL-инъекций [4]. Проведен анализ кибератак за 2018-2019 год результаты которого приведены на рисунке 1. По ОСИ - X указано количество атак, а по ОСИ - Y - месяца 2018-2019 года. Как видно из приведенных данных, эта проблема актуальна для всего мира. Киберпреступность усиливается с каждым годом, в связи, с чем возникает необходимость в применение средств защиты. Рассмотрим некоторые компании, которые предоставляют услуги по защите информации хранящиеся в БД. - IBM SecurityGuardium: она предотвращает утечки информации из баз данных, хранилищ данных и сред больших данных, таких как Hadoop, обеспечивает целостность информации и автоматизирует контроль соответствия в гетерогенных средах. Решение защищает структурированные и неструктурированные данные в базах данных, средах больших данных и файловых системах от угроз и обеспечивает соответствие требованиям.
Также предоставляет масштабируемую платформу, которая обеспечивает непрерывный мониторинг структурированного и неструктурированного трафика данных, а также применение политик для доступа к конфиденциальным данным в масштабах всего предприятия [5].
- Компания Imperva: это мировой лидер в области разработки и производства продуктов для защиты web-приложений и систем управления базами данных (СУБД). Полноценные решения позволяют производить разносторонний мониторинг и контроль над

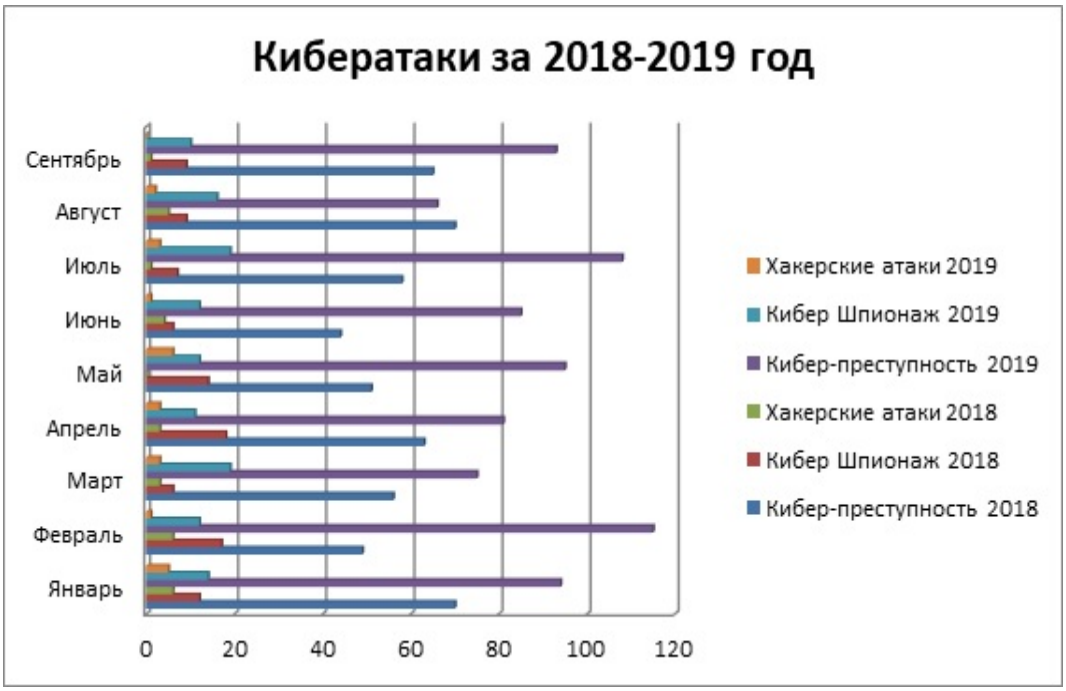


Рисунок 1: Кибератаки за 2018-2019 год

использованием всех данных и бизнес транзакций внутри дата-центра, от хранилища в базе данных или файлового сервера до использования [6].

- Imperva Database Security Secure Sphere: организации защиты важной информации в базах данных. Продукт обеспечивает комплексную прозрачность использования данных, прав доступа и уязвимостей. SecureSphere также предлагает уникальные возможности по оптимизации разворачивания решений для защиты баз данных за счет использования комбинаций удаленных сканирований и оценок, мониторинга и анализа сетевой активности с помощью программных агентов [7].

- McAfee DataCenter Security Suite for Databases: предоставляет возможность получать полную информацию об общем состоянии и уровне защищенности баз данных. Это программное решение для защиты баз данных не требует ни внесения изменений в архитектуру, ни установки дорогостоящего оборудования. В режиме реального времени решение обнаруживает и блокирует попытки атак и вторжений без необходимости отключать базы данных и тестировать приложения [8].

- McAfee Vulnerability Manager for Databases: автоматическое обнаружение базы данных, имеющиеся в вашей сети, определение установокновейших пакетов исправлений, и проводящие проверку на наличие распространенных уязвимостей [9].

- Trustwave AppDetectivePRO: сканер баз данных и хранилищ BigData, позволяющий мгновенно выявлять ошибки в конфигурации, проблемы идентификации и контроля доступа, недостающие патчи и опасные комбинации настроек, способные привести к атакам типа «повышение привилегий» или DoS-атакам, утечкам и несанкционированному изменению данных. Благодаря простой установке и интуитивно понятному интерфейсу AppDetectivePRO не требует от пользователя экспертных знаний в области баз данных.

Всего за несколько минут вы сможете мгновенно проанализировать состояние безопасности, получить оценку рисков и составить отчет о соответствии требованиям для любых БД и хранилищ BigData – как локальных, так и облачных. AppDetectivePRO является прекрасным дополнением к другим сканерам сетей и приложений [10].
- DbProtect: платформа для обеспечения безопасности данных, позволяющая мгновенно выявлять ошибки в конфигурации, проблемы идентификации и контроля доступа, недостающие патчи и опасные комбинации настроек, способные привести к атакам типа «повышение привилегий» или «отказ в обслуживании» (DoS-атакам), утечкам и несанкционированному изменению данных. За счет использования многопользовательской ролевой модели доступа и распределенной архитектуры с инструментами аналитики и отчетности корпоративного класса DbProtect защищает все реляционные СУБД и хранилища BigData в инфраструктуре компании, развернутые как локально, так и в облаке [11].
- FUDO SECURITY – ведущая польская компания, поставщик инновационных решений в области ИТ- безопасности. Компания специализируется на управлении привилегированным доступом, аутентификации и авторизации пользователей, а так же проверке зашифрованного SSL/TLS трафика [12].
- FUDO PAM – эффективное управление и контроль привилегированных пользователей. FUDO PAM – передовое решение, доступное в виде физического или виртуального устройства. Запись сессии, проактивный мониторинг на основе искусственного интеллекта, современное хранилище паролей и бизнес-аналитика – все это в одном устройстве, которое устанавливается за пару часов.
Все перечисленные компании предоставляют недешёвые услуги в связи, с чем ни каждая компания может себе позволить их приобрести. Для решения проблем связанных с безопасностью данных компании, обычно находят более выгодный и удобный вариант решения проблемы. Один из некоторых расмотрен в данной статье.

## 3 Материал и методы

Разработана модель защиты информации, хранящейся в БД. Модель отображает работу системы приложения, основанную на криптографических алгоритмах для работы с входными данными в виде файлов и потоков, хранящихся в БД. Система шифрования, обеспечивающая возможность визуализации основных процедур и проведения проверки эффективности алгоритма шифрования. Производится загрузка файла, где можно произвести выбор метода шифрования или дешифрования, следующим этапом является сохранение документа в базе данных. При работе с БД производится выбор–подключение–отображение–шифрование–сохранение и запись в БД (рисунок 2). Для предложенной модели защиты разработан алгоритм (рисунок 3).
На данной схеме представлен алгоритм описанной системы защиты информации хранящейся в базе данных.

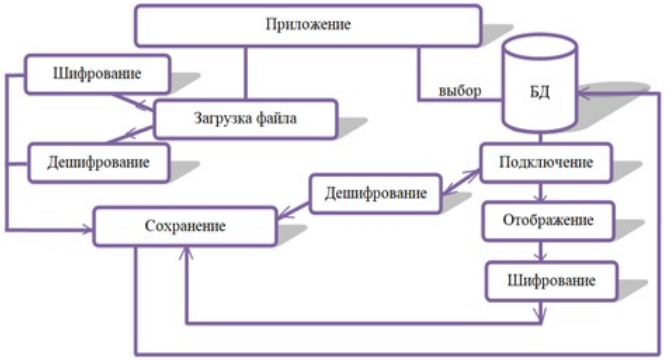


Рисунок 2: Схема работы модели защиты информации

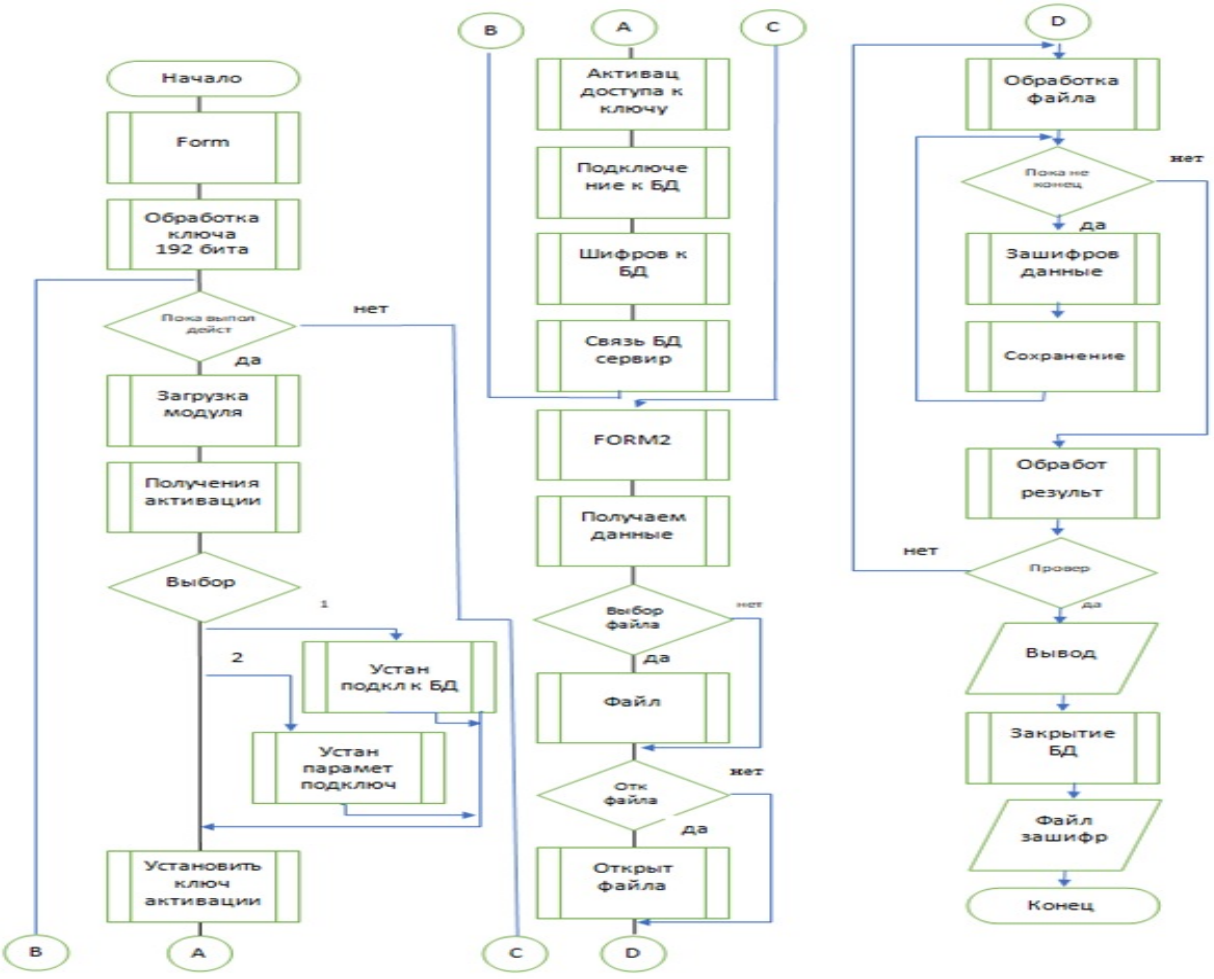


Рисунок 3: Схема работы алгоритма

## 4 Результаты и обсуждения

Программный модуль системы, обеспечивает возможность визуализации основных процедур и проведение алгоритмов проверки эффективности шифрования. Алгоритм основан на использовании криптографического метода шифрования Base64. Base64 - это механизм кодирования, используемый для представления и потоковой передачи двоичных данных через носители, ограниченные только печатными символами [13]. Основная идея технологии кодирования Base64 состоит в том, чтобы взять три символа, каждый из которых представлен в 8 битах, и превратить их в четыре символа, каждый из которых представлен в 6 битах. Получаем три символа в ASCII. Каждый символ отображается в 8-битное число от 0 до 255 на основе таблицы ASCII. Берем представление трех символов в 8 битах и соединяем их вместе, чтобы получить 24 бит. Затем разбиваем 24 бита на четыре части по 6 бит в каждой части и переводим каждую часть, используя таблицу Base64. Каждые 6 битов имеют 64 варианта символов, доступны следующие символы: цифры, строчные и прописные буквы, а также символы «+» и «/». В целом, кодировка Base64 разбивает входной текст на части по три символа и кодирует эти три символа, как описано выше. В конце процесса можно столкнуться с проблемой, когда не хватает одного или двух символов для завершения последнего трио. Чтобы решить эту проблему, кодирование добавляет один или два символа «0» в конце, чтобы создать последнюю 3-байтовую группу. Затем кодировка Base64 преобразует последние символы в '='. Поэтому иногда видим кодированный в Base64 текст, который заканчивается одним или двумя символами '='. Фиксированный префикс. Независимо от того, какая строка закодирована, после многократного кодирования в Base64 всегда получаем один и тот же фиксированный префикс, который начинается с: «Vm0wd». Причиной этого явления является то, как работает кодировка, как буква «V» ведет себя при кодировании. Кодируем букву «V» с помощью Base64. В ASCII буква «V» равна 86, что в 8-битном представлении переводится в: 01010110. После кодирования и игнорирования заполнения, поскольку нужен только префикс, берем только первые 6 бит представления, что означает 010101. В базе 64 это 21, что на удивление также является «V». Это означает, что каждый раз, когда пытаемся кодировать все, что начинается с буквы «V», получим закодированную строку, которая также начинается с «V». Это бесконечный цикл. Результат перекодировки Base64 для каждого ASCII-читаемого символа и цифры представлен на графике (рисунок 4). Каждый цвет представляет расстояние кодирования до «V»: синий - четыре итерации кодирования; зеленый - три итерации кодирования; желтый - две итерации кодирования; оранжевый - одна итерация кодирования.

Инфляция префикса. После кодирования первых трех букв фиксированного префикса остается остаток в 6 битов. Эти 6 бит будут определять следующую букву префикса. Фактически, для каждых трех букв, добавляемых к фиксированному префиксу, после кодирования остаются дополнительные 6 битов, которые будут определять дополнительный символ префикса. Это означает, что фиксированный префикс будет увеличиваться в каждой дополнительной кодировке на количество букв в префиксе, деленное на три. Например, если в фиксированном префиксе девять символов, то после другой кодировки в фиксированном префиксе будет двенадцать символов [14].

Криптографический метод позволит реализовать описанный алгоритм и будет использован в программной реализации . Программный продукт реализован под операционную

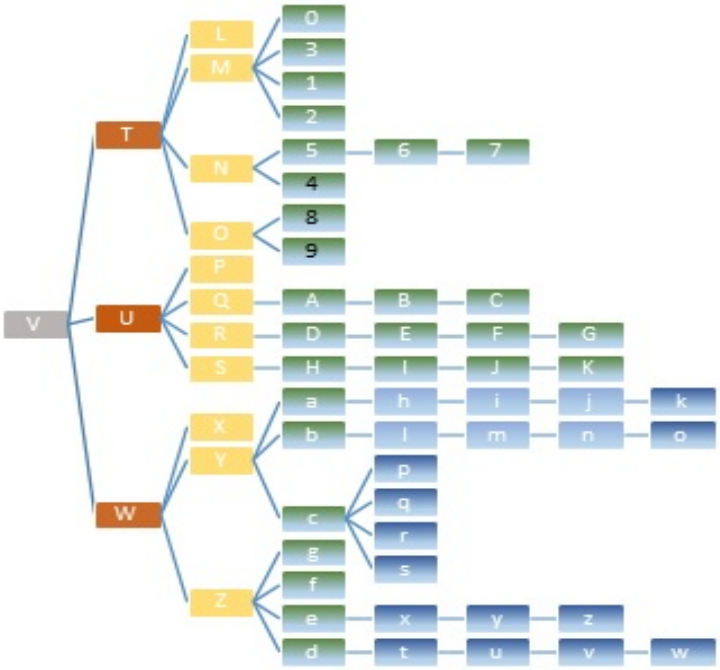


Рисунок 4: График результата перекодировки

систему Windows в среде разработки Embarcadero RAD Studio. Для работы с БД на сервере необходимо подключение к локальному серверу Firebird3. После загрузки приложения, откроется главное меню приложения, содержащее:
-в верхней части главного окна расположена кнопка «Выбор файла» для шифрования/дешифрования;
-в нижней частирасположено меню работы с БД.
Главное окно приложения представлено на (рисунок 5).

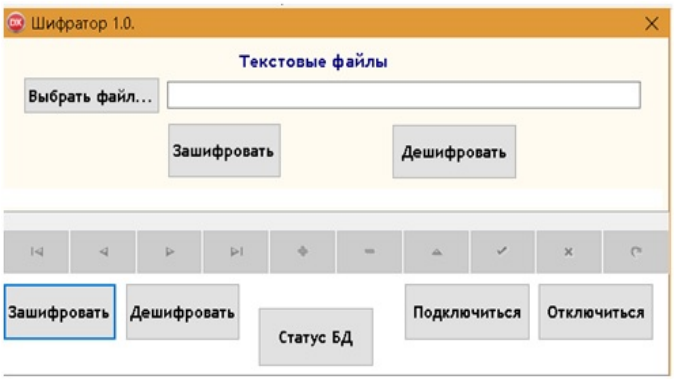


Рисунок 5: Главное окно приложения

Этапы работы приложения: При нажатии на кнопку «Выбор файла» открывается стандартное диалоговое окнодля выбора шифруемого/дешифруемого файла.

При нажатии на кнопку «Зашифровать» выбранный файл шифруется и сохраняется в той же директории с расширением *.crypt (рисунок 6).

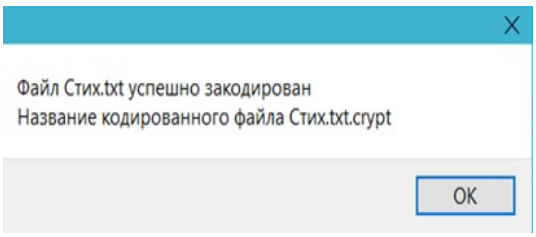


Рисунок 6: Шифрование файла

При нажатии на кнопку «Дешифровать» выбранный файл дешифруется и открывается диалоговое окно для сохранения этого файла. При нажатии на кнопку «Подключиться» появляется диалоговое окно для выбора БД. При нажатии на кнопку «Статус БД» выводится вся информация о БД, включая дату создания, размер, кол-во символов, статус зашифрована - дешифрована и т.д (рисунок 7).

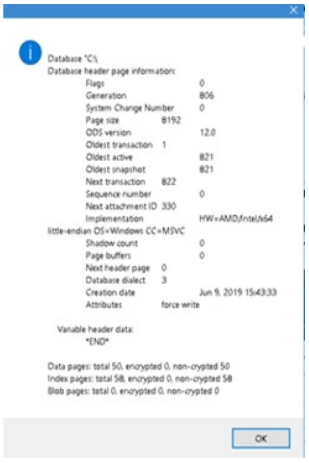


Рисунок 7: Статус базы данных

При нажатии на кнопку «Зашифровать» в выбранной БД информация зашифровывается. При повторном подключении к этой БД информация в ней не будет отображена без дешифровки,и появится окно содержащее ошибку (рисунок 8).
При нажатии на кнопку «Дешифровать» выбранная БД дешифруется и закрывается в программе. Для отображения информации требуется повторное подключение к БД. Программный продукт предназначен для зашифровывания информации и дальнейшей передачи ее по сети в закрытом виде и расшифровывании при получении ее адресатом. Особенностисоздания программы, повлиявшие на выбор языка и среды программирования.Данное приложение ориентировано в первую очередь на коммерческое использование организациями, заинтересованными в обеспечении защиты информации. Это в свою очередь, предъявляет определенные требования к интерфейсу программы. Программа

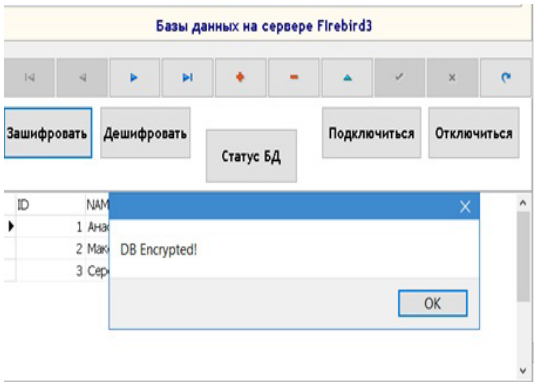


Рисунок 8: Шифрование базы данных

должна быть проста и удобна для использования. Исходя из всего вышесказанного, мы получаем вполне конкретные требования, как к языку программирования, так и к среде программирования. Всем этим требованиям удовлетворяет среда программирования Embarcadero RAD Studio используемые в ней языки программирования Deplhi и C++. Программный комплекс состоит из приложения и библиотек, необходимых для его работоспособности. Программа scrambler.exe является основным и единственным приложение с объемом 19,2M байт.
- Main.dcu 23 кб Файл с бинарным представлением основного модуля;
- CryptUnit.dcu 3кб Файл с бинарным представлением модуля Шифрования.

## 5 Заключение

В настоящий момент информационные ресурсы становятся одними из наиболее мощных инструментов экономического развития. Обладание информацией необходимых видов и качеств в нужный момент времени и в нужном месте становится залогом успеха в различных видах хозяйственно-экономической деятельности. Монопольное обладание определенными типами информацией оказывается часто одним из решающих преимуществ в конкурентной борьбе и может предопределить, таким образом, высокую цену информационных приложений. Широкое внедрение персонального компьютера выводит уровень информатизации хозяйственной жизни на качественно новые ступени. В наше время достаточно трудно обнаружить организации или предприятия (даже самые малые), которые не обладали бы современными средствами обрабатывания и передачи данных. На различных носителях данных физические и юридические лица накапливают огромные объемы информации, которая представляет большую ценность для их владельцев. Процесс создания индустрии обработки и хранения информации, хотя и создавая объективные факторы для значительного увеличения эффективности процессов деятельности человека, породил множество сложных и крупномасштабных проблем. Одна из таких проблем – это обеспечение надежного сохранения и установления статуса применения информации, которая циркулирует и обрабатывается в распределенной информационной системе. Разработанный программный модуль позволяет обеспечить целостность и конфиденциальность хранимой информации. Данный модуль - открытый

по отношению к структурам, используемым при шифровании и осуществлении операций перестановок.Данное приложение находится на стадии тестирования.

## Список литературы


[1] Послание Президента Республики Казахстан Н. Назарбаева народу Казахстана // URL: http:www.akorda.kz-ru-addresses-addresses-of -president- poslanie-prezidenta-respubliki-kazahstan-n-nazarbaeva-narodu-kazahstana-10-anvarya–2018 –g (Дата обращения 10.09.2019).

[2] Национальный доклад по науке// URL:http:nauka-nanrk.kz-ru- assets-20.pdf (Дата обращения 10.09.2019).

[3] Количество инцидентов, связанных с атаками и угрозами информационной безопасности, сократилось в сравнении с прошлым годом на 23 процента.// URL: http:www.zakon.kz-4985176-kolichestvo-intsidentov-svyazannyh-s.html (Дата обращения 21.09.2019).

[4] *Соколин Д.Т., Тимохович А.С* IМетоды комплексного обеспечения безопасности SQL – сервера от атак пита SQL – инъекций// Academy, "Автоматика. Вычислительная техника". - 2017, Т. № 3. - С.10-60.

[5] IBM Security Guardium// URL:http:www.ibm.com-security-data-security-guardium (Дата обращения 25.09.2019).

[6] Компания Imperva//URL:https:www.pacifica.kz-catalog-zashchita-bd-imperva-database-security (Дата обращения 05.10.2019).

[7] Imperva SecureSphere Data Security// URL:https:www.imperva.com-resources-datasheets-DS-SecureSphere-Data-Security.pdf (Дата обращения10.10.2019).

[8] McAfee DataCenter Security Suite for Databases // URL:https:www.mcafee. com -enterprise-en-us-assets-data-sheets-ds-data-center-security-suite-databases.pdf (Дата обращения 10.10.2019).

[9] McAfee Vulnerability Manager for Databases// URL: http:b2b-download. mcafee.com-products-evaluation-database-security-vulnerability-manager-for-databases-vmd-4.5.0-mcafee-vulnerability-manager-for-databases-product-guide-4-5.pdf (Дата обращения 13.10.2019).

[10] Trustwave AppDetectivePRO// URL:https:www.trustwave.com-en-us- resources-library- documents- trustwave-appdetectivepro (Дата обращения15.10.2019).

[11] Db Protect // URL:https:www3.trustwave.com-software-Database-Security-Db ProtectUser Guide -649.pdf (Дата обращения 15.10.2019).

[12] FUDO SECURITY// URL:https:www.fudosecurity.com (Дата обращения 26.10.2019).

[13] Base64 – принцип работы и собственная реализация// URL:http:flash2048. com- post-base64 (Дата обращения 26.10.2019).

[14] The Catch 22 of Base64: Attacker Dilemma from a Defender Point of View // URL:https://www.imperva.com/blog/the-catch-22-of-base64-attacker-dilemma-from-a-defender-point-of-view/ (Дата обращения 26.10.2019).


## References


[1] "Poslanie Prezidenta Respubliki Kazahstan N. Nazarbaeva narodu Kazahstana 10 yanvarya 2018 g."last accessed September 10, 2019., http:www.akorda.kz-ru-addresses-addresses-of -president- poslanie-prezidenta-respubliki-kazahstan-n-nazarbaeva-narodu-kazahstana-10-anvarya–2018 –g

[2] "Nacionalnyj doklad po nauke."last accessed September 10, 2019, http:nauka-nanrk.kz-ru-assets-20.pdf

[3] "Kolichestvo incidentov, svyazannyh s atakami i ugrozami informacionnoj bezopasnosti, sokratilos' v sravnenii s proshlym godom na 23 procenta."last accessed September 21, 2019, https:www.zakon.kz-4985176-kolichestvo-intsidentov-svyazannyh-s.html

[4] Sokolin D.T., Timohovich A.S., "Metody kompleksnogo obespecheniya bezopasnosti SQL – servera ot atak pita SQL – inekcij."Academy, "Avtomatika. Vychislitel'naya tekhnika"vol. 3, no 3 (2017): 10-60.

[5] "IBM Security Guardium."last accessed September 25, 2019, https:www.ibm.com-security-data-security-guardium

[6] "Kompaniya Imperva."last accessed October 10, 2019, https:www.imperva.com-resources-datasheets-DS-SecureSphere-Data-Security.pdf

[7] "Imperva SecureSphere Data Security."last accessed October 10, 2019, http:www.akorda.kz-ru-addresses-addresses-of -president- poslanie-prezidenta-respubliki-kazahstan-n-nazarbaeva-narodu-kazahstana-10-anvarya–2018 –g

[8] "McAfee DataCenter Security Suite for Databases."last accessed October 10, 2019, https:www.mcafee. com -enterprise-en-us-assets-data-sheets-ds-data-center-security-suite-databases.pdf

[9] "McAfee Vulnerability Manager for Databases."last accessed October 13, 2019, http:b2b-download. mcafee.com-products-evaluation-database-security-vulnerability-manager-for-databases-vmd-4.5.0-mcafee-vulnerability-manager-for-databases-product-guide-4-5.pdf

[10] "Trustwave AppDetectivePRO."last accessed October 15, 2019, https:www.trustwave.com-en-us-resources-library-documents-trustwave-appdetectivepro

[11] "Db Protect."last accessed October 15, 2019, https:www3.trustwave.comsoftware-Database-Security-Db ProtectUser Guide-649.pdf

[12] "FUDO SECURITY."last accessed October 26, 2019, https:www.fudosecurity.com

[13] "Base64 – princip raboty i sobstvennaya realizaciya."last accessed October 26, 2019, http:flash2048. com-post-base64

[14] "The Catch 22 of Base64: Attacker Dilemma from a Defender Point of View."last accessed October 15, 2019, https:www.imperva.com-blog-the-catch-22-of-base64-attacker-dilemma-from-a-defender-point-of-view