ТЕХНИЧЕСКИЕ НАУКИ
И ТЕХНОЛОГИИ

ТЕХНИКАЛЫҚ ҒЫЛЫМДАР МЕН ТЕХНОЛОГИЯЛАР
ТЕХНИЧЕСКИЕ НАУКИ И ТЕХНОЛОГИИ
TECHNICAL SCIENCES AND TECHNOLOGIES

DOI 10.51885/1561-4212_2023_4_186
МРНТИ 81.93.29

**Ж.З. Жантасова[1], М.А. Карменова[1], А.С. Тлебалдинова[2], А.К. Джаксалыкова[1]**
[1]Восточно-Казахстанский университет имени С. Аманжолова,
г. Усть-Каменогорск, Казахстан
*E-mail: zheniskul_z@mail.ru**
*E-mail: mmm_0582@mail.ru*
*E-mail: akmaral_s_k_87@mail.ru*
[2]Восточно-Казахстанский технический университет имени Д. Серикбаева,
г. Усть-Каменогорск, Казахстан
*E-mail: a_tlebaldinova@mail.ru*

# МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

# МӘЛІМЕТТЕР БАЗАСЫНЫҢ ҚАУІПСІЗІДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ

# DATABASE SECURITY TECHNIQUES

***Аннотация.*** *В статье отражены основные тенденции в развитии баз данных, которые порождают новые угрозы в отношении их доступности, целостности и конфиденциальности. Сделан обзор источников литературы по вопросам защиты баз данных. Описаны современные подходы к задачам обеспечения безопасности эксплуатации баз данных. Установлено соответствие между методами защиты баз данных и потенциальными угрозами, характерными для них, а также показаны источники возникновения этих угроз. На примере корпоративной информационно-образовательной системы ВКУ имени С. Аманжолова показаны реализованные элементы политики информационной безопасности: базовые механизмы обеспечения безопасности (сетевая фильтрация информационных потоков, установка антивирусного ПО), ролевая модель разграничения доступа, мандатное управление предоставлением полномочий авторизованным пользователям, журнализация действий пользователей для обеспечения процедуры неотказуемости от выполненных действий. В конце сформулированы рекомендации по расширенному использованию механизма метаданных и улучшению процедур аутентификации.*

***Ключевые слова.*** *База данных, защита и безопасность, доступность, конфиденциальность, целостность, уязвимости, потенциальные угрозы, методы и средства*

***Аңдатпа.*** *Мақалада мәліметтер базаларының қолжетімділігі, тұтастығы және құпиялығына қатысты жаңа қауіптер туғызатын даму тенденциялары көрсетілген. Мәліметтер базасын қорғау сұрақтарына қатысты дереккөздерге шолу жасалды. Мәліметтер базасын пайдаланудың қауіпсіздігін қамтамасыз ету мәселелеріне заманауи көзқарастар сипатталған. Мәліметтер базасын қорғау әдістері мен оларға тән ықтимал қауіптердің арасындағы сәйкестік орнатылды және қауіптер көздері көрсетілді. С. Аманжолов атындағы Шығыс Қазақстан университетінің корпоративтік ақпараттық-білім беру жүйесі мысалында ақпараттық қауіпсіздік саясатының жүзеге асырылуы көрсетілді: базалық қауіпсіздік механизмдері (ақпараттық ағымдардың желілік сүзілуі, антивирустық бағдарламалардың орнатылуы), ақпаратқа қатынаудың рөлдерге негізделген үлгісі, авторизацияланған пайдаланушылардың өкілеттілігін мандаттық басқару, бас тартпаушылықты қамтамасыз ету үшін пайдаланушының жүйедегі іс-әрекеттерін журналға тіркеп отыру. Мақала соңында метадеректер механизмін кеңейтіп қолдану және аутентификация процедураларын жетілдіру ұсыныстары жасалды.*

***Түйін сөздер.*** *Мәліметтер базасы, қорғау және қауіпсіздік, қолжетімділік, конфиденциалдық, тұтастық, осалдылықтар, потенциалдық қауіптер, әдіс-тәсілдер.*

***Abstract.*** *The article introduces the main trends in the development of databases that generate new threats regarding their availability, integrity and confidentiality. It provides an overview of literature sources. The article describes modern approaches to the tasks of ensuring the security of database operation. It also determines suitability database protection methods to the potential threats characteristic of them, shows the sources of these threats. Article containes example of corporate information and educational system of the East Kazakhstan University named after S. Amanzholov, where has been implemented such elements of the information security policy as basic security mechanisms (network filtering of information flows, installation of anti-virus software), role-based access control model, mandatory management of granting powers to authorized users, logging of user actions for ensuring the procedure of non-repudiation. At the end, has been formulated recommendations for the expanded use of the metadata mechanism and the improvement of authentication procedures.*

***Keywords.*** *Database, security and safety, availability, confidentiality, integrity, vulnerabilities, potential threats, methods and tools*

*Введение.* Методы хранения и применения информации в структуре баз данных продолжают оставаться основным решением в области хранения и обработки информации. При всей своей практичности, удобстве, предоставляемом СУБД для обработки запросов, подготовке аналитики для принятия решений, появляются новые потребности к эксплуатации баз данных. Это прежде всего:

– увеличение объемов хранимой информации и динамики изменения данных;

– необходимость расширения типов используемых данных (не только текст и числа, но и аудио, видео, графика, темпоральные данные, неточные данные и др.);

– совершенствование механизмов разграничения прав доступа пользователей в системе;

– совершенствование интеллектуального анализа данных;

– новые подходы к защите баз данных.

Безопасность баз данных в Интернет пространстве – важный вопрос для каждой корпоративной системы. Плохое обслуживание баз данных приводит к утечке и несанкционированному использованию конфиденциальных данных. А это, в свою очередь, может привести к потере репутации и финансовым затратам. Своевременное принятие мер по предотвращению попыток неправомерного проникновения, применение методов защиты данных в самом процессе проектирования обеспечит целостность базы данных и повысит доверие пользователей к системе.

Концепция безопасной системы в целом, базирующаяся на обеспечении доступности, целостности и конфиденциальности, вполне применима и к обеспечению безопасности баз данных, в частности. Доступность в контексте безопасности означает доступность данных, когда это необходимо авторизованным пользователям и для авторизованных целей. Чтобы обеспечить доступность система должан быть защищена от прерывания работы и ухудшения качества обслуживания. Целостность данных связана с согласованными данными, то есть достоверными, без ошибок и аномалий. С точки зрения безопасности организационных процессов пользователи должны поддерживать целостность на всех уровнях внутри организации, при этом должна обеспечиваться проверка данных. Процесс проверки целостности охватывает и ввод данных, и хранение, обработку, использование и архивирование. Конфиденциальность защищает данные от разглашения любой информации, которая нарушает права человека или организации. Различают уровни конфиденциальности информации, например, «совершенно секретно», «секретно», «в открытом доступе». Политика информационной безопасности (ИБ) регулирует соответствие соблюдения

пользователями требуемых уровней конфиденциальности.

Целью данного исследования является систематизация современных подходов к решению задач безопасности баз данных (БД). Определены следующие задачи исследования:

– обзор методов и технологий защиты БД (литературный обзор);

– установление соответствия методов защиты баз данных потенциальным угрозам, характерным для баз данных, а также указание источников их возникновения;

– описание политики информационной безопасности, реализованной в организации;

– выработка рекомендаций по расширенному использованию механизма метаданных и улучшению процедур аутентификации.

*Литературный обзор.* Авторы учебников и учебных пособий по БД нередко затрагивают вопросы обеспечения баз данных, однако детального рассмотрения вопросов встречается очень редко. Так, в учебном пособии [1] авторы, рассматривая систему безопасности в СУБД SQL Server, подразделяют ее на 2 уровня: серверный и уровень баз данных. На уровне сервера выделяют идентификацию, аутентификацию, ролевую политику разграничения доступа как меры по защите сервера. Авторы [2] также придерживаются этих двух уровней обеспечения безопасности БД и определяют компоненты систем безопасности на рассматриваемых уровнях. На уровне сервера функционирует система аутентификации средствами Windows и средствами SQL Server, используются учетные записи пользователей и встроенные роли сервера. Идентификация же пользователей баз данных, пользовательские роли БД, роли приложений обеспечиваются на уровне базы данных.

Фундаментальная работа Кристофера Дейта формирует уникальное толкование терминов, принятых в теории баз данных, разъясняя расхождения толкований в повседневной жизни и публикациях. Так, он пишет «Вопросы защиты данных часто рассматриваются вместе с вопросами поддержки целостности данных (по крайней мере, в неформальном контексте), хотя на самом деле это совершенно разные понятия» [3]. Термин защита относится к защищенности данных от несанкционированного доступа, изменения или умышленного разрушения, а целостность – к точности или достоверности данных. Под защитой данных подразумевается предотвращение доступа к ним со стороны несанкционированных пользователей. Под поддержкой целостности подразумевается предотвращение их разрушения при доступе со стороны санкционированных пользователей. Автор, однако, не исключает сходства между рассматриваемыми понятиями, так как в обоих случаях происходит проверка на корректность выполняемых пользователями установленных ограничений. При этом вопросы поддержки целостности данных рассматриваются отдельно в силу фундаментальности понятия [3-4]. А вопросы защиты данных получают особую актуальность в силу его практической важности в условиях повсеместного распространения Интернета, электронной коммерции и разворачивающегося на этом фоне интернет-мошенничества. В данном контексте прежде всего предлагаются избирательная и мандатная модели разграничения доступа. В первом случае, доступ и полномочия относительно какого либо объекта выбираются владельцем объекта по своему усмотрению. При этом может быть использован механизм модификации запроса, а для регистрации нарушения – контрольный журнал. В мандатной, более жесткой модели, каждый объект должен обладать уровнем конфиденциальности (метки безопасности), а каждый субъект – определенным уровнем допуска. Соответственно, каждый субъект получает допуск к объекту не ниже своего уровня допуска. Интересным, как нам кажется, подход автора к защите статистических баз данных. Как правило, такие БД

содержат большое количество конфиденциальных данных, но при этом пользователям может предоставляться только некоторая статистически обобщенная информация. Реальной угрозой таких БД являются средства слежения, что особо вызывает тревогу в связи с интересом к хранилищам данных. Одним из подходов в данном случае является шифрование данных. К полезным рекомендациям можно отнести использование представлений для сокрытия информации и применение операторов языка SQL – GRANT и REVOKE для контроля наборами полномочий, предоставленных конкретным пользователям в отношении различных объектов базы данных (в основном это базовые таблицы и представления) [4].

Последовательное рассмотрение вопросов защиты, связанных с проектированием, реализацией и сопровождением баз данных, рассматривается Коннолли Т., Бегг К. [5]. Классификация типов угроз, механизм представлений, особенности защитных механизмов в средах различных СУБД: управление транзакциями, методы блокировки, восстановления, методы защиты СУБД в Web подробно излагаются авторами.

В контексте защиты баз данных понимается комплекс организационных, программных и технических методов и средств, направленных на удовлетворение ограничений, установленных для типов данных или экземпляров типов данных в системах обработки данных [6]. Как видим из данного определения, автор исходит из фундаментального толкования обеспечения целостности данных. Защита данных включает предупреждение случайного или несанкционированного доступа к данным, их изменения или разрушения со стороны пользователей или при сбоях аппаратуры. Реализация защиты включает контроль целостности данных с помощью ограничений, обеспечение физической целостности данных, секретности данных.

Кузнецов С.Д. – специалист в области системного программирования и баз данных, профессор МГУ имени М. Ломоносова, является автором фундаментальных трудов в области баз данных. Наравне с различными подходами к концепции реализации баз данных в его трудах можно увидеть совершенно новые потенциальные возможности к обеспечению безопасности баз данных. Прежде всего это, хэширование, BASE-транзакции для распределенных систем (в отличие от ACID-транзакции для классических СУБД), способы восстановления данных [7-8].

Общая идея хэширования связана с ключом поиска, хэш-функция или функция свертки выдает значение меньшего размера, которое используется для доступа к требуемой записи.

ACID-транзакция, как механизм обеспечения целостности, характеризуется следующими свойствами атомарности (Atomicity), согласованности (Consistency), изолированности (Isolation) и долговечности (Durability). В распределенных системах ACID-транзакцию обеспечить практически невозможно, здесь применяется модель BASE, которая поддерживает следующие свойства:

– Базовая доступность (basic availability);

– Гибкое состояние (soft state);

– Согласованность в конечном счете (eventual consistency).

На сегодняшний день в базах данных сосредоточены большие объемы информации, что лишение доступа может стоить для компании потенциально разрушительных потерь. Требование надежного хранения, возможность восстановления согласованного состояния после аппаратных и программных сбоев, одно из важных требований к эксплуатации СУБД. База данных может быть повреждена или уничтожена в результате пожара, взрыва, землетрясения, что также делает критически важными процедуры резервного копирования и восстановления.

Очевидно, для обеспечения этих требований необходима некоторая избыточная информация, которая в СУБД поддерживается в виде журнала изменений баз данных.

Ситуации, приводящие к необходимости восстановления состояния базы данных, могут быть следующие:

1) Индивидуальный откат транзакции. Это либо завершение транзакции оператором Rollback, либо откат инициируется системой на исключительную ситуацию, например, деление на ноль;

2) Восстановление после внезапной потери содержимого оперативной памяти. Например, вследствие отключения электропитания;

3) Восстановление после прихода в негодность внешнего носителя базы данных. Эта ситуация при достаточно высокой надежности современных устройств внешней памяти может происходить редко, но, тем не менее, СУБД должна иметь возможность восстановления данных и в этом случае. Основой восстановления служат архивная копия и журнал изменений базы данных.

Вопросы обеспечения безопасности баз данных автором Мамедли Р.Э. рассмотрена прежде всего с позиции защиты данных от случайного или преднамеренного использования посторонними пользователями [9]. В базе данных основной акцент делается на информацию как на ценный ресурс, потеря которого чревата серьезным ущербом для деятельности компании. И здесь прослеживается требование строгого соответствия всей деятельности организации процедурам обеспечения доступности, целостности и конфиденциальности. Также следует отметить рассмотрение авторами уязвимостей и соответствующих мер безопасности на шести уровнях: пользователей, серверов, операционных систем, приложений, сети и данных. Безусловно, большее количество рассматриваемых уровней позволяет более детально подходить и к выбору мер безопасности.

*Материалы и методы исследования.* Понятие безопасной системы требует комплексного подхода в масштабах всей организации. Это означает невозможность защиты данных без защиты всех процессов и систем вокруг этих данных. Это и аппаратные системы, программные приложения, сетевое оборудование, внутренние и внешние пользователи, процедуры и собственно, сами данные.

Для каждой из составляющей компоненты безопасной системы есть подходящие методы и средства. Подбор и реализация тех или иных способов защиты вытекает из перечня потенциальных угроз и анализа уязвимостей в системе.

Типичными уязвимостями БД являются:

1) наличие в системе прав и полномочий, остающихся при увольнении либо перемещении сотрудника из одной должности в другую. Такие случаи могут быть источниками утечки информации или несанкционированных изменений в БД;

2) наличие в системе пользователей с расширенным регламентом прав и привилегий. В этой ситуации возможны злоупотребление своими полномочиями, что также могут привести к различным инцидентам;

3) SQL и NoSQL инъекции: проникновение через определенные вредоносные коды, что позволяет злоумышленниками манипулировать данными;

4) Различные кибератаки и заражение вирусами. Это могут быть и подмены данных, и массовые рассылки вредоносных ссылок, и доступ к конфиденциальным данным и т.д.;

5) Отсутствие регулярного аудита и мониторинга специалистов, контролирующих доступ к сведениям критической важности;

6) Отсутствие регулярных обновлений в системе.

Анализ угроз, потенциально имеющих опасность для функционирования системы

поддержки БД, облегчает возможность выбора тех или иных методов защиты. Авторами данной работы подготовлена таблица, показывающая взаимосвязь различных видов угроз, характерных для баз данных, их источники, а также перечень рекомендуемых при этом методов и средств обеспечения безопасности (табл. 1).

**Таблица 1.** Наиболее характерные угрозы и методы защиты БД

| Наименование потенциальной угрозы | Источник угрозы | Нарушаемый компонент безопасной системы | Перечень методов и средств защиты |
|---|---|---|---|
| Ошибки при вводе данных | Операторы, непрофессиональные пользователи | целостность | Триггеры, транзакция, ограничения целостности |
| Аномалии обновления | Корректировка данных связанных таблиц | целостность | Механизм ссылочной целостности, транзакция |
| Технические сбои | Скачки напряжений в сети, перегрузка | доступность | 1. Установка источников бесперебойного питания<br>2. Резервное копирование и восстановление |
| Утечка информации | SQL и NoSQL инъекции | Конфиденциальность | Разграничение доступа внутри системы, аутентификация, шифрование, тестирование ПО |
| Несанкционированный доступ | SQL и NoSQL инъекции | Конфиденциальность, целостность | Разграничение доступа внутри системы, аутентификация, шифрование, Web Application Firewall (WAF), тестирование ПО |
| «Слабое» администрирование | Кадровый потенциал, отсутствие политики ИБ | доступность | Аудит и мониторинг, периодическое обновление версий и конфигураций БД, повышение квалификации сотрудников |
| «Отказ в обслуживании» | 1. Атаки переполнения буфера<br>2. DoS, DDoS – атаки<br>3. Вирусные атаки | доступность | 1. Использование брандмауэров,<br>2. Составление списка контроля доступа (ACL),<br>3. Устанавливать лицензионные приложения<br>4. Устанавливать антивирусное обеспечение<br>5. Пентест<br>6. Использование VPN |

*Результаты и их обсуждения.* В данном разделе описаны основные подходы, реализованные в политике информационной безопасности ВКУ имени С.Аманжолова. Политика как как документированная процедура СМК, регламентирующая цели и задачи обеспечения ИБ в вузе, разработана, утверждена и действует с 2013 года. Корпоративная информационно-образовательная система (КИОС) ВКУ имени С. Аманжолова состоит из следующих основных модулей-подсистем: Сайт вуза (vku.edu.kz/), образовательный портал (edu.vku.edu.kz/), портал сопровождения обучения и контроля знаний обучающихся (euniver.vku.edu.kz/). Также есть дополнительные подсистемы, поддерживающие учебный процесс и административные функции: научная библиотека (https://library.vku.edu.kz/), корпоративная почта (https://mail.vku.edu.kz/mail/), разработка и сопровождение рабочих и учебных планов, расчет педнагрузки (http://ais.vku.edu.kz/),

электронный документооборот (https://docflow.vku.edu.kz).

Одним из базовых механизмов, применяемых для фильтрации сетевых потоков в образовательную среду вуза является установка и настройка межсетевого аппаратно-программного комплекса. Благодаря ему все информационные потоки из вне контролируются на предмет соответствия требованиям регламентированных сетевых протоколов. В настоящее время это стандартное требование к корпоративным средам. Приобретено и установлено лицензионное антивирусное программное обеспечение, обеспечивается периодическое обновление антивирусных баз.

Во всех модулях системой предусмотрена аутентификация пользователей. Процедура подтверждения подлинности пользователя основана на ролевой политике разграничения доступа (RBAC), где основные роли распределены между ролью обучающегося и преподавателя. Есть контролирующие управленческие роли (ректор, проректора, деканы факультетов и заведующие кафедр, руководители структурных подразделений), а также оперативные роли (разработчики рабочих учебных планов (эдвайзеры), администраторы сети, разработчики ПО) и др. После успешной аутентификации пользователя активность действий поддерживается элементами мандатной политики полномочий, где каждый объект доступа имеет определенную метку конфиденциальности («доступа нет», «доступно для просмотра», «доступна корректировка»). Каждый авторизованный субъект также имеет соответствующий установленный уровень доступа. При попытке субъекта получить доступ к защищенному объекту реализуется процедура выявления соответствия уровня доступа субъекта метке конфиденциальности объекта. При успешной верификации процедуры предоставляется доступ, соответствующий метке конфиденциальности. Также в системе предусмотрен регламент времени активности субъекта. Выход за пределы установленного регламента влечет повторную процедуру аутентификации.

В отдельных случаях возникает необходимость достоверного подтверждения точечных манипуляций пользователя, позволяющего обеспечить неотказуемость от выполненных действий в системе. Например, в период экзаменационной сессии, обучающиеся могут предъявлять претензии к нестабильности работы портала в момент сдачи компьютерного тестирования. При подаче на апелляцию приложение, разработанное программистами центра информационно-технического обеспечения и цифровизации университета, позволяет получить статистику действий данного обучающегося в момент сдачи экзамена. Результат статистики позволяет специалистам академического департамента либо удовлетворить апелляцию и дать возможность повторной сдачи экзамена в случае технических сбоев в момент экзамена. Либо доказать факт академической нечестности, допущенной со стороны апеллирующего обучающегося. Таким образом, в данном случае, реализуемая процедура безопасности оказывает содействие принятию правильного управленческого решения.

Следует отметить, что все процедуры обеспечения безопасности информационной системы в целом, в том числе и систем хранения и обработки данных, интегрированы во все рабочие процессы реальной системы и целенаправленны на предупреждение инцидентов, связанных с доступностью, целостностью и конфиденциальностью данных.

В целом деятельность в рамках обеспечения безопасности КИОС вуза направлена на создание полностью верифицируемой системы, где все защитные процедуры подтверждают соответствие событий, регистрируемых в системе, всем установленным процедурам политики безопасности. Одно из направлений работы в контексте предоставления достоверных данных является работа с метаданными. В связи с тем, что все больше информации сохраняется и используется в цифровом формате, необходимы такие средства хранения и воспроизведения, которые не подвержены «старению» и способны

правильно интерпретировать информацию. В целом, человечество нуждается в средствах хранения, поддерживающих неограниченный во времени доступ к данным в полезной для использования форме. Одним из механизмов реализации этой задачи является наличие метаданных, описывающих контекст, при отсутствии которых и доступные данные могут быть бесполезными. То есть, вместе с хранимыми данными должны быть и описывающие эти данные метаданные. Подобные идеи метаданных сейчас используются при архивировании публикаций журналов, для обеспечения доступа к ним, а также для принятия, рецензирования и допуска к публикации материалов авторов.

Системы аутентификации, гарантирующие прохождение в рабочую среду санкционированных пользователей, имеют свои пробелы. Многофакторная аутентификация позволяет в какой-то степени восполнить эти пробелы. Однако, в перспективе, более надежные механизмы могут быть выработаны на основе формальных методов верификации с математическими техниками спецификаций, технологий темпоральной логики.

Таким образом, в данной статье предпринята попытка комплексного анализа вопросов защиты баз данных. Для этого выявлены наиболее характерные уязвимости систем обработки данных, потенциальные угрозы по отношению ко всем процессам, связанным с созданием, поддержкой и сопровождением баз данных. Также установлена взаимосвязь уязвимостей, угроз и необходимых мер по обеспечению безопасности баз данных. Дано описание реализованных методов защиты информации и достигнутых результатов на примере корпоративной информационно-образовательной среды ВКУ имени С. Аманжолова (КИОС). Авторами статьи определены новые вызовы по отношению к обеспечению безопасности баз данных.

*Выводы.* Достигнутые в исследовании авторов результаты могут быть использованы и в других подобных информационно-образовательных средах, а также полезны для продолжения проводимой работы, обеспечив комплексный подход к политике ИБ в масштабах всей организации. Можно рекомендовать результаты и в качестве учебных ресурсов при преподавании в вузе курсов по защите информации.

Список литературы


1. Куандыкова Д.Р., Утепбергенов И.Т., Хомоненко А.Д. Ақпараттық жүйелердегі деректер қорының теориясы мен тәжірибесі. Оқу құралы. – Алматы: «Тұран» университеті, 2017. – 256 б.
2. Игнатьева О.В. Прикладное программирование и базы данных: учебно-методическое пособие для практических работ / О.В. Игнатьева; ФГБОУ ВО РГУПС. – Ростов н/Д, 2017. – 206 с.
3. К.Дж.Дейт Введение в системы баз данных. Учебник. 8-е издание.: Пер. с англ. — М.: Издательский дом «Диалектика», 2019. – 1328 с.: ил. – Парал. тит. англ.
4. Осипов Д.Л. Технологии проектирования баз данных. – М.: ДМК Пресс, 2019. – 498 с., ил.
5. Коннолли Т. Базы данных. Проектирование, реализация и сопровождение. Теория и практика: пер. с англ. / Т.Коннолли, К.Бегг. - М. и др.: Вильямс, 2017. - 1439 с.
6. Карпова И.П. Базы данных. Учебное пособие. М.: Питер, 2020 – 240 с.
7. Кузнецов С. Д. Базы данных. Лекции ученых МГУ. https://vk.com/teachinmsu - 256 с.
8. Онлайн образовательный портал МГУ имени М.Ломоносова: https://teach-in.ru/
9. Мамедли Р.Э. Системы управления базами данных: Учебное пособие. – Нижневартовск: Издательство Нижневартовского государственного университета, 2021. – 214 с.
10. http://citforum.ru/database/
11. Тлебалдинова А.С., Жұртпаева А.Ә., Жантасова Ж.З. Мәліметтер базасын жобалаудың заманауи технологиялары. Оқу құралы. Усть-Каменогорск, ВКГУ им. С. Аманжолова, Издательство «Берел», 2019. – 136 с.
12. Жантасова Ж.З., Акказин А., Тлебалдинова А.С., Увалиева И.М. Мәліметтерді интеллектуалды жүйелер көмегімен іздеу. // Вестник ВКГТУ. – 2019. – №3(85). – С.75-78.
13. Жантасова Ж.З., Тлебалдинова А.С., Жұртпаева А.Ә. Қолданбалы бағдарламалау және деректер қоры. Оқу құралы. Издательство «Берел» ВКУ им. С.Аманжолова.-2019.-142 с.
14. Жантасова Ж.З., Джаксалыкова А.К. Oracle ортасында мәліметтер базасымен жұмыс жасау:

Метод. указания.– Усть-Каменогорск: ВКГУ им.С.Аманжолова, Изд-во «Берел», 2017. – 79 с.
15. https://rt-solar.ru/products/solar_dozor/blog/2719/
16. Kuznetsov, S.D. Towards a native architecture of In-NVM DBMS.- Proceedings – 2019. Actual Problems of Systems and Software Engineering, APSSE 2019, 2019, pp. 77–89, 8943792. https://orcid.org/0000-0002-8257-028X
17. Toapanta, Moisés & Escalante Quimis, Omar & Mafla, Enrique & Maciel, Rocio. (2020). Analysis for the Evaluation and Security Management of a Database in a Public Organization to Mitigate Cyber Attacks. IEEE Access. 8. 18. 10.1109/ACCESS.2020.3022746.
18. Yesin, V., Karpinski, M., Yesina, M., Vilihura, V., Warwas, K. Ensuring Data Integrity in Databases with the Universal Basis of Relations. Appl. Sci. 2021, 11, 8781. https:// doi.org/10.3390/app11188781
19. Sarbeswar H., Pravat S. DataBase Security by applying AES Algorithm: A Review. International Journal of Advanced Research in Engineering and Technology (IJARET) Volume 11, Issue 11, November 2020, pp.1809-1814, Article ID: IJARET_11_11_168Available online at ttp://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=11ISSN Print: 0976-6480 and ISSN Online: 0976-6499DOI: 10.34218/IJARET.11.11.2020.168
20. Wang, Y., Xi, J.S. and Cheng, T. (2021) The Overview of Database Security Threats' Solutions: Traditional and Machine Learning. Journal of Information Security, 12, 34-55. https://doi.org/10.4236/jis.2021.121002

References

1. Kuandykova D.R., Utepbergenov İ.T., Homonenko A.D. Aqparattyq jüielerdegı derekter qorynyñ teoriasy men täjıribesı. Oqu qūraly. - Almaty: «Tūran» universitetı, 2017 – 256 bet.
2. Ignat'eva O.V. Prikladnoe programmirovanie i bazy dannyh: uchebno-metodicheskoe posobie dlya prakticheskih rabot / O.V. Ignat'eva; FGBOU VO RGUPS. – Rostov n/D, 2017. – 206 s.
3. K.Dzh.Dejt Vvedenie v sistemy baz dannyh. Uchebnik. 8-e izdanie.: Per. s angl. – M.: Izdatel'skij dom "Dialektika", 2019. – 1328 s.: il. – Paral. tit. angl.
4. Osipov D.L. Tekhnologii proektirovaniya baz dannyh. – M.: DMK Press, 2019. – 498 s., il.
5. Konnolli T. Bazy dannyh. Proektirovanie, realizaciya i soprovozhdenie. Teoriya i praktika: per. s angl. / T.Konnolli, K.Begg. - M. i dr.: Vil'yams, 2017. – 1439 s.
6. Karpova I.P. Bazy dannyh. Uchebnoe posobie. – M.: Piter, 2020. – 240 s.
7. Kuznecov S.D. Bazy dannyh. Lekcii uchenyh MGU. https://vk.com/teachinmsu - 256 s.
8. Onlajn obrazovatel'nyj portal MGU imeni M.Lomonosova: https://teach-in.ru/
9. Mamedli R.E. Sistemy upravleniya bazami dannyh: Uchebnoe posobie. – Nizhnevartovsk: Izdatel'stvo Nizhnevartovskogo gosudarstvennogo universiteta, 2021. – 214 s.
10. http://citforum.ru/database/
11. Tlebaldinova A.S., Jūrtpaeva A.Ä., Jantasova J.Z. Mälımetter bazasyn jobalaudyñ zamanaui tehnologialary. Oqu qūraly. Üst-Kamenogorsk, VKGU im.S.Amanjolova, İzdatelstvo «Berel», 2019.-136 s.
12. Jantasova J.Z., Akkazin A., Tlebaldinova A.S., Uvalieva İ.M. Mälımetterdı intelektualdy jüieler kömegımen ızdeu. // Vestnik VKGTU. – 2019. – № 3(85). – S. 75-78.
13. Jantasova J.Z., Tlebaldinova A.S., Jūrtpaeva A.Ä. Qoldanbaly bağdarlamalau jäne derekter qory. Oqu qūraly. İzdatelstvo «Berel» VKU im. S.Amanjolova. – 2019. – 142 s.
14. Jantasova J.Z., Jaksalykova A.K. Oracle ortasynda mälımetter bazasymen jūmys jasau. Metodicheskie ukazania. Üst-Kamenogorsk, VKGU im. S. Amanjolova, İzdatelstvo «Berel», 2017. – 79 s.
15. https://rt-solar.ru/products/solar_dozor/blog/2719/
16. Kuznetsov, S.D. Towards a native architecture of In-NVM DBMS.- Proceedings – 2019. Actual Problems of Systems and Software Engineering, APSSE 2019, 2019, pp. 77–89, 8943792. https://orcid.org/0000-0002-8257-028X
17. Toapanta, Moisés & Escalante Quimis, Omar & Mafla, Enrique & Maciel, Rocio. (2020). Analysis for the Evaluation and Security Management of a Database in a Public Organization to Mitigate Cyber Attacks. IEEE Access. 8. 18. 10.1109/ACCESS.2020.3022746.
18. Yesin, V., Karpinski, M., Yesina, M., Vilihura, V., Warwas, K. Ensuring Data Integrity in Databases with the Universal Basis of Relations. Appl. Sci. 2021, 11, 8781. https:// doi.org/10.3390/app11188781
19. Sarbeswar H., Pravat S. DataBase Security by applying AES Algorithm: A Review. International Journal of Advanced Research in Engineering and Technology (IJARET) Volume 11, Issue 11, November 2020, pp.1809-1814, Article ID: IJARET_11_11_168Available online at ttp://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=11ISSN Print: 0976-6480 and ISSN Online: 0976-6499DOI: 10.34218/IJARET.11.11.2020.168

20. Wang, Y., Xi, J.S. and Cheng, T. (2021) The Overview of Database Security Threats' Solutions: Traditional and Machine Learning. Journal of Information Security, 12, 34-55. https://doi.org/10.4236/jis.2021.121002