Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.056:004.77

Герман
Евгений Васильевич

СИСТЕМА БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ НА ОСНОВЕ СУБД MS SQL SERVER 2017

АВТОРЕФЕРАТ
диссертации на соискание степени магистра

по специальности 1-39 80 03 Электронные системы и технологии (профилизация «Компьютерные технологии проектирования электронных систем»)

Минск 2021

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **БОНДАРИК Василий Михайлович,**

кандидат технических наук, доцент, декан факультета непрерывного и дистанционного обучения учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **ПОЛОЗКОВ Юрий Владимирович,**

кандидат технических наук, доцент, заведующий кафедрой «Программное обеспечение вычислительной техники и автоматизированных систем» БНТУ

Защита диссертации состоится «24» июня 2021 г. года в 9^{00} часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, E-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

В современных условиях деятельность любой организации сопряжена с оперированием большим объемом информации, доступ к которой имеет широкий круг лиц. Следствием возросшего в последнее время значения информации стали высокие требования к конфиденциальности, целостности и доступности данных. В таких условиях злонамеренные или просто некомпетентные действия всего лишь одного из сотрудников организации способны нанести непоправимый ущерб организации в целом. Речь даже может не идти о хищении ценной информации. Достаточно просто заблокировать какими-либо средствами доступ к важному информационному ресурсу на достаточно продолжительное время.

Системы управления базами данных (СУБД), в особенности реляционные СУБД, стали доминирующим инструментом в области хранения, обработки и представления данных. Любой сбой в работе СУБД, сопровождающийся потерей, хоть и временной, доступа к данным, немедленно отражается на конкурентной способности предприятия. Поэтому защита данных от несанкционированного доступа, от несанкционированной модификации или просто от их разрушения является одной из приоритетных задач при проектировании любой информационной системы. Проблема защиты данных охватывает как физическую защиту данных и системных программ, так и защиту от несанкционированного доступа к данным, передаваемым по линиям связи и находящимся на накопителях, являющегося результатом деятельности как посторонних лиц, так и специальных программ-вирусов. Если принять во внимание, что ядром информационной системы является СУБД, то обеспечение информационной безопасности последней приобретает решающее значение при выборе конкретных средств обеспечения необходимого уровня безопасности организации в целом.

Данные в компьютерной форме сосредоточивают в физически локальном и небольшом объеме (например, на флэш-карте типа MicroSD) огромные массивы информации, несанкционированный доступ к которой или ее разрушение могут приводить порой к катастрофическим последствиям и ущербу. Возможность быстрого (и в отдельных случаях даже без следов) копирования, модификации или удаления огромных массивов данных, находящихся в компьютерной форме, в том числе и удаленно расположенных, дополнительно провоцирует злоумышленников на несанкционированный доступ к информации, ее модификацию или разрушение.

В современных БД довольно успешно решаются задачи защиты конфиденциальных данных от несанкционированного доступа, обеспечения целостности и доступности данных. Обеспечение доступности данных на физическом уровне достигается путем использования отказоустойчивых устройств хранения данных, например, нескольких жестких дисков,

объединенных в массив RAID. Периодическое создание резервных копий и хранение результатов всех операций в файле журнала позволяет восстановить данные практически после любого сбоя. Целостность данных обеспечивается довольно широким набором процедур, обеспечивающим достоверность и непротиворечивость данных. Современные СУБД обеспечивают логическую целостность и непротиворечивость данных уже на этапе описания модели данных. Операторы контроля доступа входят в стандарт языка запросов SQL и реализованы во многих СУБД. Но все же, несмотря на широкий диапазон средств контроля и защиты, общий уровень защищенности и СУБД и ЭС определяется возможностями используемой операционной системы, поскольку эти два компонента работают в тесной связи между собой.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

По мере того как деятельность организаций все больше зависит от компьютерных информационных технологий, проблемы защиты баз данных становятся все более актуальными. Угрозы потери конфиденциальной информации стали обычным явлением в современном компьютерном мире. Если в системе защите есть недостатки, то данным может быть нанесен ущерб, который может быть выражен в: нарушении целостности данных, потере важной информации, попадании важных данных посторонним лицам и т.д.

Степень разработанности проблемы

Исследование защиты информации в базах данных осуществлялось с использованием работ российских и белорусских ученых: С.Н. Смирнов, В. Л. Цирлов, В.А Герасименко и др.

Одним из недостатков исследований, представленных в современной технической литературе, является неполное рассмотрение особенностей и условий комплексной защиты информации.

Цель и задачи исследования

Целью диссертации является исследование архитектуры системы безопасности СУБД MS SQL SERVER 2017. В ней рассмотрены: специфика защиты в базах данных, восстановление целостного состояния базы данных, а также система безопасности уровня сервера и система безопасности уровня баз даных.

Поставленная цель работы определяет **следующие основные задачи:**

1. Провести обзор и анализ современного состояния проблемы. Рассмотреть специфику защиты информации в базах данных, дискреционное разграничение доступа и ролевое разграничение доступа.

2. Разработать методику восстановления целостного состояния базы данных и организацию восстановления данных. Рассмотреть различные методы восстановления, достоинства и недостатки этих методов, создание отказоустойчивых систем.

3. Исследовать архитектуру системы безопасности уровня сервера и уровня базы данных. Разработать SQL запросы, которые позволят развивать стратегию всесторонней защиты информации корпоративной сети на основе СУБД MS SQL SERVER 2017.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) ОСВО 1-39 80 03-2019 специальности 1-39 80 03 Электронные системы и технологии (профилизация «Компьютерные технологии проектирования электронных систем»).

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в таких областях, как защита информации, система корпоративной сети и СУБД MS SQL SERVER 2017.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна и значимость полученных результатов работы заключается в разработке методики моделирования защиты корпоративной сети.

Теоретическая значимость работы заключается в выделении концептуальных направлений, в рамках которых должна вестись защита инфорамации предприятия.

Практическая значимость диссертации состоит в разработке SQL запросов, которые позволят развивать стратегию всесторонней защиты с перекрывающимися уровнями безопасности для повышения общего уровня безопасности корпоративной сети и уменьшить потери минимум на 20%.

Основные положения, выносимые на защиту

1. Анализ современного состояния проблемы. Специфика защиты информации в базах данных, дискреционное разграничение доступа и ролевое разграничение доступа.

2. Восстановления целостного состояния базы данных и организация восстановления данных. Рассмотрены различные методы восстановления, достоинства и недостатки этих методов, создание отказоустойчивых систем

3. Архитектура системы безопасности уровня сервера и уровня базы данных. SQL запросы, которые позволят развивать стратегию всесторонней

защиты информации корпоративной сети на основе СУБД MS SQL SERVER 2017.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе приведена специфика защиты информации в базах данных, а также рассмотрены идентификация и аутентификация пользователей, авторизация пользователей, дискреционное разграничение доступа и ролевое разграничение доступа.

Во второй главе представлены принципы и методы восстановления данных, а также восстановления данных в СУБД MS SQL SERVER и создание отказоустойчивых систем.

В третьей главе рассмотрена архитектура системы безопасности уровня сервера и уровня базы данных. SQL запросы, которые позволят развивать стратегию всесторонней защиты информации корпоративной сети на основе СУБД MS SQL SERVER 2017.

В приложении представлены публикации автора.

Общий объем диссертационной работы составляет 71 страницf. Из них 51 страницf основного текста, 1 иллюстрации на 1 странице, 2 таблицы на 1 странице, библиографический список из 50 наименований на 4 страницах, 3 приложений на 21 странице.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы защиты информации корпоративной сети, указаны основные направления исследований, проводимых по данной тематике, а также описано обоснование актуальности темы.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе приведен обзор современного состояния проблемы защиты информации в базах данных. Также рассмотрены идентификация и аутентификация пользователей, авторизация пользователей, дискреционное разграничение доступа и ролевое разграничение доступа.

Установлено, что некоторые СУБД поддерживают списки разрешенных идентификаторов пользователей и паролей, отличающиеся от аналогичного списка, поддерживаемого ОС. Другие типы СУБД поддерживают списки, элементы которых приведены в соответствие существующим спискам пользователей операционной системы и выполняют регистрацию, исходя из текущего идентификатора пользователя, указанного им при регистрации в системе. Это предотвращает попытки пользователей зарегистрироваться в СУБД под идентификатором, отличным от того, который они пользовали при

регистрации в системе. Управление доступом есть метод защиты информации путем регулирования использования ресурсов системы (элементов БД, программных и технических средств). Включает следующие функции защиты:

- идентификация пользователей и ресурсов системы;
- установление подлинности объекта или субъекта по предъявленному им идентификатору (аутентификация);
- разграничение и проверка полномочий (авторизация), создание условий работы в пределах установленного регламента;
- регистрация обращений к защищаемым ресурсам (протоколирование и аудит);
- реагирование при попытках несанкционированного доступа.

На практике может применяться комбинированный способ управления доступом, когда определенная часть полномочий на доступ к объектам устанавливается администратором, а другая часть владельцами объектов. Некоторыми объектами в среде СУБД владеет сама СУБД. Обычно это владение организуется посредством использования специального идентификатора особого суперпользователя – например, с именем system administrator.

Пользователи могут быть объединены в специальные группы пользователей. Один пользователь может входить в несколько групп. Для пользователей с минимальным стандартным набором прав вводится понятие группы PUBLIC. По умолчанию предполагается, что каждый вновь создаваемый пользователь, если специально не указано иное, относится к группе PUBLIC. Если СУБД поддерживает использование идентификаторов как отдельных пользователей, так и их групп, то, как правило, идентификатор пользователя будет иметь более высокий приоритет, чем идентификатор группы.

Наиболее распространенный вид информационных угроз заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно самая главная проблема определить, кто и к каким наборам данных должен иметь доступ, а кто нет. Другими словами, необходимо определить термин «несанкционированный». По характеру, воздействия НСД является активным воздействием, использующим ошибки системы. НСД обращается обычно непосредственно к требуемому набору данных, либо воздействует на информацию о санкционированном доступе с целью легализации НСД. НСД может быть подвержен любой объект системы. НСД может быть осуществлен как стандартными, так и специально разработанными программными средствами к объектам. Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует ИС, так и для ее пользователей. На рисунке 1 представлены последствия нарушения системы безопасности, а на рисунке 2 представлена зависимость снижения потерь после внедрения СЗИ.

Рисунок 1 – Последствия нарушения безопасности

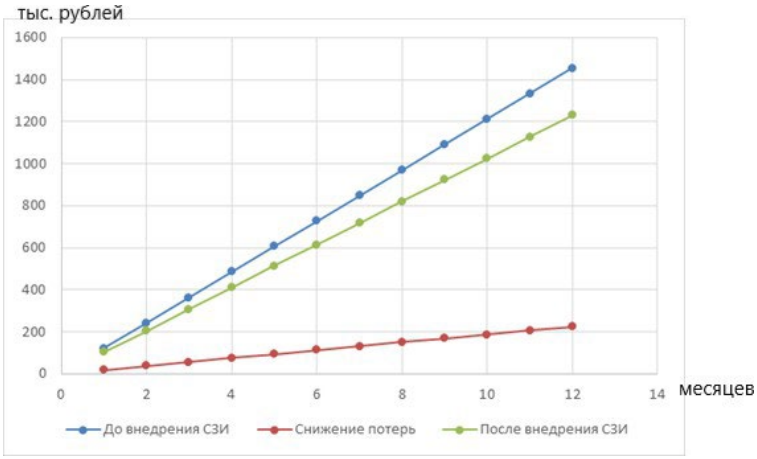

Рисунок 2 – Снижение потерь после модернизации системы защиты информации

Во второй главе рассмотрены способы методы и принципы восстановление данных. А также понятие транзакции и создание отказоустойчивых систем.

Установлено, что SQL Server предлагает на выбор три модели восстановления, в основном отличающихся использованием журнала

транзакций, и пять вариантов резервного копирования. Модели восстановления следующие:

1 Простая модель. Журнал транзакций не резервируется (не создает-

ся его резервная копия во внешней памяти).

2 Модель с неполным протоколированием. Массовые операции не заносятся в журнал транзакций. Журнал транзакций резервируется.

3 Полная модель. Все транзакции заносятся в журнал. Журнал транзакций резервируется.

Резервное копирование возможно следующих видов:

1 Полное. Резервируются все данные.

2 Дифференцированное. Производится резервирование всех страниц данных, измененных с момента последнего полного резервного копирования.

3 Журнала транзакций. Производится резервирование всех транзакций в журнале.

4 Файла или файловой группы. Производится резервирование всех данных, содержащихся в файле или файловой группе.

5 Файловое дифференцированное. Производится резервирование всех страниц данных, модифицированных с момента последнего резервного копирования файла или файловой группы.

Восстановление всегда начинается с использования полной резервной копии. После этого из архивов дифференцированного и транзакционного резервирования восстанавливаются все транзакции, выполненные с момента создания полной резервной копии. Модель восстановления конфигурирует настройки базы данных SQL Server таким образом, чтобы обеспечить тот тип восстановления, который необходим базе данных. Ключевые отличия между разными моделями восстановления связаны с тем, в какой мере в них задействован журнал транзакций и какие данные в нем регистрируются.

Простая модель восстановления идеально подходит тем базам данных, которым требуется обеспечение атомарности транзакций, но не обязательна поддержка их живучести. Простая модель форсирует очищение сервером баз данных журнала в контрольных точках. При этом журнал будет хранить транзакции, запись которых в базу данных еще не подтверждена. Пространство же, отведенное для хранения всех остальных транзакций, освобождается для повторного использования. Так как журнал транзакций в этой модели является только временным местом хранения, отпадает потребность в его резервировании. Эта модель восстановления имеет ряд преимуществ. Во-первых, журнал транзакций имеет маленькие размеры, однако расплачиваться за это придется потерей всех транзакций, выполненных с момента последнего полного или дифференцированного резервирования. План восстановления, основанный на простой модели, позволяет выполнять полное резервирование раз в неделю, а дифференцированное – в конце каждого дня недели. Полная и дифференцированные резервные копии заменяются, когда будет выполнено следующее полное резервное копирование.

Соответственно, восстановление в простой модели предполагает две операции:

- восстановление из последней полной резервной копии;
- восстановление из последней (не обязательно) одной дифференцированной резервной копии.

Полная модель восстановления предлагает наиболее грубый и надежный план восстановления. В этой модели все транзакции, в том числе и массовые операции, протоколируются в журнале. Любая системная функция, такая как создание индекса, также протоколируется. Основным преимуществом этой модели является то, что все транзакции, выполненные в базе данных, могут быть восстановлены, вплоть до момента, предшествовавшего системному сбою. К недостаткам следует отнести медленное выполнение массовых операций, очень большой размер файла журнала транзакций и более длительное время выполнение операций резервирования и восстановления журнала транзакций.

Полная модель восстановления может использовать все пять типов резервирования базы данных. Чаще всего полная модель восстановления предполагает выполнение полного резервирования дважды в неделю, а дифференцированного – в конце каждого дня. Резервирование журнала транзакций выполняется регулярно на протяжении всего дня, при этом промежутки времени между отдельными сессиями могут колебаться от нескольких часов до нескольких минут. Восстан овление базы данных в этой модели предполагает выполнение следующих операций:

- восстановление из последней полной резервной копии;
- восстановление из последней дифференцированной резервной копии, созданной после выполнения последнего полного резервирования (если таковая имеется);
- восстановление всех резервных копий журнала транзакций, созданных с момента последнего полного или дифференцированного резервного копирования.

Если последней созданной резервной копией была полная, то ее восстановления будет достаточно. Если последней созданной резервной копией была дифференцированная, то перед ее восстановлением следует выполнить восстановление из последней полной резервной копии.

В третьей главе рассмотрена архитектура системы безопасности MS SQL SERVER 2017 уровня сервера и уровня баз данных. А также показаны SQL запросы для системы безопасности уровня сервера и уровня базы данных.

Использование аутентификации Windows означает, что пользователю для доступа к SQL Server достаточно иметь учетную запись Windows. Идентификатор безопасности Windows передается из операционной системы на сервер баз данных. SQL Server предполагает, что процесс регистрации пользователей в сети достаточно защищен, и поэтому не выполняет никаких дополнительных проверок. Пользователь автоматически получает соответствующие права доступа к данным SQL Server сразу же после регистрации в домене. Такой метод предоставления доступа называется установлением доверительного соединения. Операционная система работает с

учетными записями (logins), которые содержат все данные о пользователе, включая его имя, пароль, членство в группах, каталог по умолчанию и т. д. Каждая учетная запись имеет уникальный идентификатор (Login ID) или, как его называют по-другому, идентификатор безопасности (SID, Security Identification), с помощью которого пользователь регистрируется в сети.

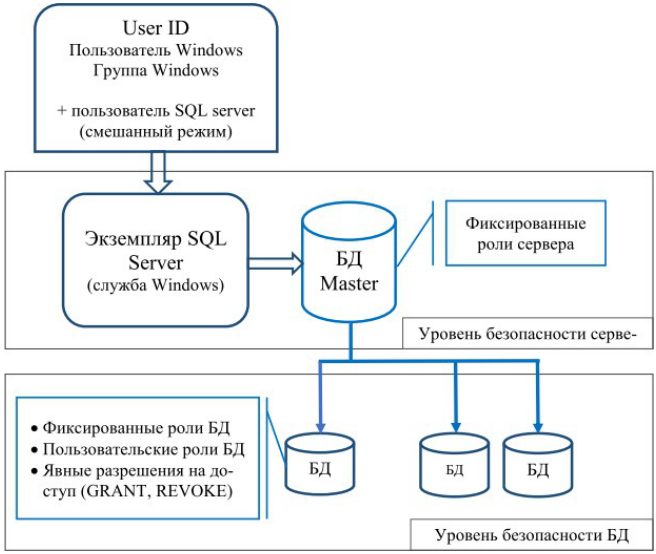

Рисунок 1 – Обобщенная схема безопасности СУБД MS SQL Server

Аутентификация Windows предусматривает сохранение в системной базе данных Master только идентификационного номера учетной записи пользователя в домене SID. Информация об имени пользователя, его пароле и т. д. хранится в базе данных домена. Изменение имени пользователя или его пароля никак не отразится на правах доступа к SQL Server. Информация об учетной записи пользователя и его членстве в группах Windows считывается SQL Server из базы данных системы безопасности домена во время подключения пользователя. Если администратор внес какие-то изменения в учетную запись пользователя, например, исключил его из некоторой группы, то изменения отразятся только во время очередной регистрации пользователя в домене или в SQL Server в зависимости от категории сделанных изменений.

Аутентификация Windows дает определенные преимущества. На пользователях автоматически отражаются все правила политики безопасности, установленные в домене. Пользователю не приходится запоминать еще один пароль. Это повышает уровень общей защищенности данных. Например, автоматически контролируется минимальная длина пароля и срок его действия. Операционная система требует от пользователя периодической смены пароля. Дополнительно можно запретить пользователям установку паролей, уже указывавшихся ранее. Кроме того, Windows имеет встроенные средства защиты от подбора паролей. Аутентификация Windows работает также с группами

пользователей. Когда имя группы Windows передается в SQL Server в качестве регистрационной записи, любой член этой группы может быть аутентифицирован сервером баз данных. SQL Server также известно истинное имя пользователя Windows, входящего в группу, вследствие чего приложение может выполнять аудит на уровне пользователей, а также на уровне групп пользователей.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Проведен обзор и анализ современного состояния проблемы. Рассмотрена специфика защиты информации в базах данных, дискреционное разграничение доступа и ролевое разграничение доступа.

2. Разработана методика восстановления целостного состояния базы данных и организацию восстановления данных. Рассмотрены различные методы восстановления, достоинства и недостатки этих методов, создание отказоустойчивых систем.

3. Исследована архитектуру системы безопасности уровня сервера и уровня базы данных. Разработаны SQL запросы, которые позволят развивать стратегию всесторонней защиты информации корпоративной сети на основе СУБД MS SQL SERVER 2017 и уменьшат потери минимум на 20%.

Рекомендации по практическому использованию результатов

Полученные результаты можно использовать в любой корпоративной сети, любом предприятии и государственном учреждении.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Тезисы конференций

1. Герман, Е.В. Решение проблемы отвода тепла при корпусировании полупроводниковых приборов и микросхем / Е.В. Герман, Е.В. Гармилин, С.А. Ефименко, В.М. Бондарик // Электронные системы и технологии: сборник материалов 57-й научной конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, 19–23 апреля 2021 г. / редкол.: Д. В. Лихачевский [и др.]. – Минск: БГУИР, 2021. – С. 443-446.

2. Герман, Е.В. Измерение тепловых сопротивлений силовых полупроводниковых приборов / Е.В. Герман, Е.В. Гармилин, С.А. Ефименко, В.М. Бондарик // Электронные системы и технологии: сборник материалов 57-й научной конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, 19–23 апреля 2021 г. / редкол.: Д. В. Лихачевский [и др.]. – Минск: БГУИР, 2021. – С. 447-450.

РЭЗЮМЭ

Герман Яўген Васільевіч

СІСТЭМА БЯСПЕКІ КАРПАРАТЫЎНАЙ СЕТКІ НА АСНОВЕ СУБД MS SQL SERVER 2017

Ключавыя словы: сістэма бяспекі, СКБД, MS SQL SERVER 2017.

Мэта працы: даследаванне архітэктуры сістэмы бяспекі СКБД MS SQL SERVER 2017.

Атрыманыя вынікі і іх навізна: Праведзены агляд і аналіз сучаснага стану праблемы. Разгледжана спецыфіка абароны інфармацыі ў базах дадзеных, аднамернай размежаванне доступу, ролевае размежаванне доступу. Распрацавана методыка аднаўлення цэласнага стану базы дадзеных і арганізацыя аднаўлення дадзеных. Разгледжаны розныя метады аднаўлення, вартасці і недахопы гэтых метадаў, стварэнне адказаўстойлівы сістэм. Даследавана архітэктура сістэмы бяспекі ўзроўню сервера і ўзроўню базы дадзеных. Распрацаваны SQL запыты, якія дазволяць развіваць стратэгію ўсебаковай абароны інфармацыі карпаратыўнай сеткі на аснове СКБД MS SQL SERVER 2017 і паменшыць страты мінімум на 20%.

Ступень выкарыстання: Атрыманыя вынікі можна выкарыстоўваць у любой карпаратыўнай сеткі, любым прадпрыемстве і дзяржаўнай установе.

Вобласць ужывання: Любыя прадпрыемствы і дзяржаўныя ўстановы.

РЕЗЮМЕ

Герман Евгений Васильевич

СИСТЕМА БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ НА ОСНОВЕ СУБД MS SQL SERVER 2017

***Ключевые слова*:** система безопасности, СУБД, MS SQL SERVER 2017.

***Цель работы*:** исследование архитектуры системы безопасности СУБД MS SQL SERVER 2017.

***Полученные результаты и их новизна*:** Проведен обзор и анализ современного состояния проблемы. Рассмотрена специфика защиты информации в базах данных, дискреционное разграничение доступа, ролевое разграничение доступа. Разработана методика восстановления целостного состояния базы данных и организация восстановления данных. Рассмотрены различные методы восстановления, достоинства и недостатки этих методов, создание отказоустойчивых систем. Исследована архитектура системы безопасности уровня сервера и уровня базы данных. Разработаны SQL запросы, которые позволят развивать стратегию всесторонней защиты информации корпоративной сети на основе СУБД MS SQL SERVER 2017 и уменьшить потери минимум на 20%.

***Степень использования*:** Полученные результаты можно использовать в любой корпоративной сети, любом предприятии и государственном учреждении.

***Область применения*:** Любые предприятия и государственные учреждения.

SUMMARY

German Evgeny Vasilievich

The method for ensuring the functional reliability of electronic modules based on microcontrollers when exposed to static discharges electricity

***Keywords*:** security system, DBMS, MS SQL SERVER 2017.

***The object of study*:** study of the architecture of the security system of the MS SQL SERVER 2017 DBMS.

***The results and novelty*:** A review and analysis of the current state of the problem is carried out. The specifics of information security in databases, discretionary access control, role-based access control are considered. A method for restoring the integrity of the database and organizing data recovery has been developed. Various recovery methods, advantages and disadvantages of these methods, creation of fault-tolerant systems are considered. The architecture of the security system at the server and database levels has been investigated. SQL queries have been developed that will allow developing a strategy for comprehensive protection of corporate network information based on the MS SQL SERVER 2017 DBMS and reduce losses by at least 20%.

***Degree of use*:** The results obtained can be used in any corporate network, any enterprise and government agency.

Sphere of application: Any enterprises and government agencies.