. Администрирование баз данных

Цель занятия: усвоить знания о порядке такой организации работы пользователей с базой данных, чтобы база данных всегда была работоспособна.

**План**

1. Функции администратора БД.
2. Методы защиты БД.
3. Резервирование и восстановление БД.
4. Оптимизация работы БД,
5. Правовая охрана баз данных
6. Функции администратора бд

Использование автоматизированных информационных систем порождает общие информационные ресурсы в виде базы или совокупности баз данных, состояние и функционирование которых может критически влиять на жизнедеятельность предприятия, организации. В результате, как и для любого критического ресурса, требуются отдельное специфическое управление и контроль состояния, получившие в процессе внедрения АИС в практику информационного обеспечения деятельности предприятий и организаций специальный термин — «администрирование и защита данных (баз данных)».

В номенклатуре специалистов, обеспечивающих проектирование, создание, эксплуатацию и использование АИС, соответственно, выделилась отдельная категория, называемая «администраторами систем (баз данных)», играющих ключевую роль в процессах информационного обеспечения деятельности предприятий и организаций.

Взгляды на функции и содержание задач, решаемых в процессе администрирования баз данных, формировались вместе со становлением индустрии АИС, менялись вместе с изменениями и усложнениями программно-технических аспектов реализации АИС. Но постепенно сформировался некоторый их базовый перечень, и администрирование баз данных вошло неотъемлемым ключевым компонентом в теорию и практику автоматизированных информационных систем.

Термин «**администрирование**» определяет комплекс процессов при создании, эксплуатации и использовании АИС, связанных с обеспечением надежности и эффективности функционирования АИС, безопасности данных и организацией коллективной работы пользователей различных категорий.

Этот комплекс процессов можно разделить по решаемым задачам на следующие группы:

* обеспечение и поддержание настройки структурного, интерфейсного и технологического компонентов АИС на структуру и процессы предметной области системы;
* обеспечение надежности и сохранности данных;
* организация и обеспечение коллективной работы пользователей с общими данными.

Первое направление обусловливает участие администратора системы в этапах проектирования и ввода АИС в эксплуатацию. Администратор при этом выступает **экспертом** в команде разработчиков по выбору СУБД и ее особенностям в плане реализации тех или иных компонент концептуальной схемы создаваемого банка данных, участвует в процессах создания типовых запросов, экранных форм для ввода и вывода данных, шаблонов отчетов. На этапе проектирования и, в особенности, в процессе дальнейшей эксплуатации при наполнении системы данными администратор системы производит анализ адекватности и эффективности спроектированной внутренней схемы базы данных и при необходимости может осуществлять ее корректировку. Для обеспечения таких функций некоторые СУБД содержат специальный программный инструментарий в виде анализаторов быстродействия и оптимальности баз данных.

В эту же группу функций входит создание и поддержание словарно-классификационной базы (словари, справочники, ключевые слова, тезаурусы), которая должна адекватно отражать особенности предметной области информационной системы.

Еще одной важной функцией, особенно на этапе ввода информационной системы в эксплуатацию, является **первоначальное наполнение системы данными**. Во многих случаях для этого могут быть использованы данные из других информационных систем, находящихся, возможно, в других физических форматах и с другой логической организацией. Импорт данных из внешних источников, как правило, требует высокой квалификации по возможностям используемой в АИС СУБД, детального представления логической и физической организации данных в АИС и выполняется вследствие этого администратором системы. В фактографических АИС на основе реляционных СУБД подобные задачи решаются на основе запросов на создание таблиц, источник данных для которых находится во внешних базах или в файлах других форматов (электронные таблицы, текстовые файлы). Соответственно, особенности функционирования АИС могут требовать решения и обратных задач, то есть задач экспорта данных во внешние системы и другие форматы. Такие задачи в большинстве случаев также решаются администраторами АИС.

Обеспечение **надежности и сохранности** данных является одной из главных обязанностей администратора АИС и включает, в свою очередь, решение ряда следующих технологических и профилактических задач:

* планирование, конфигурирование и поддержание системы использования устройств внешней памяти, на которых размещаются файлы данных;
* архивирование и резервирование данных;
* восстановление данных после сбоев и повреждений;

• проверка и поддержание целостности данных.

Большой объем файлов баз данных, как уже отмечалось, обусловливает их размещение на устройствах дисковой (внешней) памяти. Поэтому отдельной задачей при проектировании АИС является определение **схемы размещения файлов** базы данных системы на устройствах внешней памяти, контроль за ее состоянием в процессе эксплуатации АИС.

В перечень функций администратора по обеспечению восстановления данных входит также **профилактика дисковых носителей*внешней памяти****,*обеспечиваемая специальными программными инструментальными утилитами операционной системы — проверка состояния дисков, дефрагментация и т. д. Данные обязанности накладывают дополнительные требования к профессиональной подготовке администраторов как особого направления подготовки системных программистов.

**Проверка и поддержание целостности данных**является также неотъемлемой функцией администраторов и заключается в обеспечении настройки и функционирования защитных механизмов СУБД поддерживающих ограничения целостности данных и связей в конкретной базе данных. Как правило, в большинстве СУБД имеются встроенные механизмы автоматического поддержания и контроля целостности данных. Вместе с тем, в ряде случаев, логика предметной области не дает возможности устанавливать такие режимы обеспечения целостности связей, как, например, каскадное обновление и удаление связанных записей. При этом в процессе работы пользователей с базой данных может образовываться множество коллизий в виде «оборванных» связей, что снижает эффективность функционирования базы данных. В таких ситуациях одной из функций администратора базы данных являются периодический контроль целостности связей и устранение подобных коллизий. В некоторых СУБД для решения этих задач предусмотрены специальные режимы и механизмы «ревизии» и восстановления целостности базы данных. В других СУБД данные задачи решаются через технику запросов или через разработку, в том числе и самими администраторами АИС специальных программных утилит.

Сходные задачи ревизии данных решаются администратором также в тех случаях, когда устанавливаются временные https://studfiles.net/html/2706/1067/html_wK6mevxKd_.zBh9/img-4NFDyD.pngрегламенты хранения данных и устаревшие данные должны своевременно обновляться или удаляться из системы.

Большой комплекс функций администратора АИС связан с ***организацией и обеспечением*коллективной работы пользователей*с общими данными.***Еще на этапе проектирования АИС с непосредственным участием будущего администратора системы разрабатывается организационная схема функционирования и использования АИС. Исходя из особенностей технологических процессов в предметной области и круга решаемых задач, определяются функциональные группы работников, отвечающих за ввод, обработку и использование общих данных системы. На этой основе строится перечень и схема пользователей системы, определяются их конкретные функции, полномочия, разрабатываются необходимые технологические и интерфейсные элементы (входные и выходные экранные формы, запросы, шаблоны отчетов и т. д.), прорабатываются и устанавливаются внутренние параметры и характеристики коллективной обработки данных (размещение данных, параметры блокировок, обмена и т. д.). Администратор АИС, по сути, является как раз организатором и руководителем этих технологических процессов организации работы эксплуатационного персонала и абонентов-пользователей системы.

Отдельным, но тесно переплетенным с остальными функциями, направлением этого комплекса обязанностей администратора системы является ***создание и поддержание системы разграничения доступа к данным и*защиты данных*от несанкционированного доступа****.*На основе системы и схемы функций, задач и полномочий пользователей и обслуживающего персонала администратором строится и поддерживается схема категорирования объектов базы данных по критерию доступа различных пользователей и внешних процессов, осуществляется текущее управление этой схемой и аудит процессов обработки данных с точки зрения безопасности и разграничения доступа к данным.

Развитые СУБД в составе своих функций и возможностей, как правило, имеют специальный *инструментарий, обеспечивающий основной набор функций и задач администратора*— уже упоминавшийся анализатор быстродействия и оптимальности, утилиты архивирования, резервирования и ревизии базы данных, подсистему разграничения доступа и защиты данных.

В настольных однопользовательских системах, строящихся на основе СУБД с развитым интерфейсным набором инструментов по созданию и управлению базами данных, все или большая часть функций администратора может выполняться самими пользователями, которые в необходимых случаях могут лишь изредка прибегать к помощи и консультациям соответствующих специалистов. Вместе с тем рассмотренный перечень функций и решаемых задач, так или иначе, реализуется и в однопользовательских системах.

Следует также отметить, что организационно администраторы АИС являются отдельными штатными категориями работников информационных служб, подчиняясь непосредственно руководителям таких служб, или во многих случаях, собственно, и выполняя функции руководителя службы информационного обеспечения предприятия, организации, отдельного подразделения.

# Методы защиты бд

Одной из оборотных сторон компьютерных информационных технологий является обострение *проблемы защиты информации.*Данные в компьютерной форме сосредоточивают в физически локальном и небольшом объеме огромные массивы информации, несанкционированный доступ к которой или ее разрушение могут приводить порой к катастрофическим последствиям и ущербу. Возможность быстрого, во многих случаях практически мгновенного, и без следов копирования огромных массивов данных, находящихся в компьютерной форме, в том числе и удаленно расположенных, дополнительно *провоцирует злоумышленников*на несанкционированный доступ к информации, ее несанкционированную модификацию или разрушение.

Вместе с тем теоретическая проработка вопросов обеспечения безопасности информации и их практическая реализация долгое время отставали от уровня развития программной индустрии СУБД и в коммерческих продуктах средства обеспечения безопасности данных стали появляться лишь в 90-х годах.

В настоящее время рождается технология защиты информации в ИС и КС. Основные угрозы безопасности:

* раскрытие конфиденциальной информации (несанкционированный доступ);
* компрометация информации (искажение или уничтожение);

Импульсы развития и первые исследования теории и практики обеспечения безопасности данных в компьютерных системах были обусловлены, прежде всего, потребностями военной сферы, где проблема безопасности в целом, и компьютерной безопасности в частности стоят особенно остро. Начало этим процессам было положено исследованиями вопросов защиты компьютерной информации, проведенными в конце 70-х — начале 80-х годов национальным центром компьютерной безопасности (NCSC - National Computer Security Center) Министерства обороны США. Результатом этих исследований явилось издание Министерством обороны США в 1983 г. документа под названием *«****Критерии оценки надежных компьютерных систем****»,*впоследствии по цвету обложки получившего название *«Оранжевой книги».*Данный документ стал фактически первым стандартом в области создания защищенных компьютерных систем и впоследствии основой организации системы сертификации компьютерных систем по критериям защиты информации.

Подходы к построению и анализу защищенных систем, представленные в «Оранжевой книге», послужили методологической и методической базой для дальнейших исследований в этой сфере. В 1991г. NCSC был издан новый документ - *Интерпретация «Критериев оценки падежных компьютерныхсистем» в применении к попятит падежной системы управления базой данных,*известный под сокращенным названием TDI или «Розовой книги», конкретизирующий и развивающий основные положения «Оранжевой книги» по вопросам создания и оценки защищенных СУБД.

В конце 80-х - начале 90-х годов аналогичные исследования по проблемам компьютерной безопасности были проведены во многих странах и созданы соответствующие национальные стандарты в этой сфере. В Беларуси в декабре 2007 г. принят в первом чтении закон «О защите информации»,определяющий требования, методику и стандарты построения защищенных компьютерных сетей и автоматизированных информационных систем.

**Технологии идентификации и аутентификации** являются обязательным элементом защищенных систем, так как обеспечивают принцип персонализации субъектов и, тем самым, реализуют *первый (исходный) программно-технический рубеж защиты информации*в компьютерных системах.

Под ***идентификацией***понимается различение субъектов, объектов, процессов по их образам, выражаемым именами.

Под *аутентификацией*понимается проверка и подтверждение подлинности образа идентифицированного субъекта, объекта, процесса.

Часть *угроз безопасности*информации возникает из-за непреднамеренных (или преднамеренных) *ошибок на этапах жизненного цикла АИС* - при разработке программного обеспечения СУБД; при проектировании и создании на базе СУБД конкретной АИС, и, в том числе, при проектировании системы разграничения доступа; при администрировании и сопровождении системы и, в том числе, при реагировании и действиях пользователей во внештатных ситуациях; при технологических операциях по резервированию, архивированию и восстановлению информации после сбоев; при выводе АИС из эксплуатации. С целью нейтрализации или снижения вероятности данных угроз применяются ряд организационно-технологических и технических средств, решений, объединяемых в общую группу ***технологий*надежного проектирования и администрирования**.Их также условно можно разделить на следующие подгруппы:

* + технологии надежной разработки программного обеспечения;
    - технологии надежного проектирования и создания АИС;
  + технические средства и специальный инструментарий администрирования АИС;

Администратор безопасности организует и управляет системой разграничения доступа — доверительные характеристики (допуска) пользователей, конкретные назначения доступа, регистрация и формирование меток доступа пользователей.

Доступ к массиву учетных **записей пользователей имеет только администратор безопасности. Совмещение функций общего администрирования и администрирования безопасности одновременно одним пользователем не допускается, что объективно повышает надежность системы.**

Технические средства и специальный инструментарий администрирования АИС применяются для создания условий и возможностей восстановления данных после всевозможных сбоев, обеспечения более эффективной работы АИС.

**Протоколирование и аудит** событий безопасности являются важным средством обеспечения управляемости состоянием и процессами безопасности, создают условия для расследования фактов нарушения информационной безопасности, анализа и исключения их причин, снижения отрицательных последствий и ущерба от них.

Документированию подлежат все события, критичные с точки зрения безопасности в системе:

* вход/выход пользователей;
* регистрация новых пользователей, смена привилегий и назначений доступа (все обращения к массивам учетных записей);
* все операции с файлами (создание, удаление, переименование, копирование, открытие, закрытие);
* обращения к/из удаленной системе (ы).

При этом по каждому такому событию устанавливается минимально необходимый перечень регистрируемых параметров, среди которых:

* дата и время события;
* идентификатор пользователя-инициатора;

# Резервирование и восстановление бд

В ряде приложений сохранность и работоспособность базы данных является чрезвычайно критическим аспектом либо в силу технологических особенностей (системы реального вре**https://studfiles.net/html/2706/1067/html_wK6mevxKd_.zBh9/img-OmBzm7.pnghttps://studfiles.net/html/2706/1067/html_wK6mevxKd_.zBh9/img-kP8aqg.png**мени), либо в силу содержательного характера данных. В этих случаях применяются подходы так называемого ***горячего резервирования***данных, когда база данных постоянно находится в виде двух идентичных (зеркальных) и параллельно функционирующих копий, размещаемых на двух раздельных системах дисковой памяти.

В других ситуациях для обеспечения сохранности данных используются операции ***архивирования и резервирования данных****.*В большинстве случаев архивирование производится обычными средствами архивации файлов для их компактного долговременного хранения, как правило, на внешних съемных носителях. Функции архивирования данных иногда могут входить и в перечень внутренних функций самих СУБД.

Резервирование данных, как правило, не предусматривает специального сжатия данных, а производится через создание специальных копий файлов данных в технологических или иных целях.

И архивирование, и резервирование, помимо технологических целей, преследуют также профилактические цели по еще одной чрезвычайно важной операции, выполняемой администратором АИС — восстановлению*данных после сбоев и повреждений.*Наличие резервной или архивной копии базы данных позволяет восстановить работоспособность системы при выходе из строя основного файла (файлов) данных. При этом, однако, часть данных, или их изменений, произведенные за время, прошедшее с момента последнего архивирования или резервирования, могут быть потеряны. Такие ситуации особенно критичны при коллективной обработке общих данных, реализуемых клиент-серверными системами. Поэтому в промышленных СУБД, реализующих технологии «Клиент-сервер», в большинстве случаев предусматривается ведение специального журнала текущих изменений базы данных, размещаемого отдельно от основных данных и, как правило, на отдельном носителе. Как уже отмечалось, такой подход называется**журнализацией**. В журнале изменений осуществляются непрерывная фиксация и протоколирование всех манипуляций пользователей с базой данных. В результате при любом сбое с помощью архивной копии и журнала изменений администратор системы может полностью восстановить данные до момента сбоя посредством **отката-наката** операций транзакций по журналу текущих изменений базы данных.

## Оптимизация работы бд

У каждого производителя базы данных есть целый раздел в документации, который посвящен вопросам производительности и оптимизации работы базы данных. Надо понимать, что типовая поставка базы данных обычно подразумевает минимальное серверное оборудование, минимальную память и диски. То есть стандартные конфигурации не учитывают возможности конкретного оборудования и конкретного приложения. Поэтому надо обязательно настраивать базу данных для обеспечения оптимальной работы.

Основные принципы оптимизации:

* **как можно меньше дисковых операций чтения данных;**надо увеличивать размер буфера кэширования, чтобы база данных как можно меньше читала данные с диска;
* **как можно меньше сортировок данных на диске;**надо увеличить буфер сортировки таким образом, чтобы избежать двойных сортировок и сортировок на диске.
* **увеличивать параллельность исполнения запросов**за счет запуска большого числа процессов базы данных, выбора форматов хранения данных, обеспечивающих параллельность работы;
* **отложенная фиксация транзакций на диске;**очень желательно настроить базу данных так, чтобы при изменении данных или их вставке не производилась немедленная запись на диск, а изменения собирались и фиксировались с некоторым интервалом; это позволяет значительно быстрее возвращать управление продукту после выполнения SQL запросов;

Сервер базы данных - это сложное приложение и обязательно нужно изучить документацию поставщика по вопросам настройки.

Важным параметром, влияющим на потребление памяти базами данных, является максимальное число одновременных соединений. Поэтому надо стремиться уменьшить число одновременных соединений и высвободить больше памяти для сортировки данных в памяти и буферизации.

# Правовая охрана баз данных

1. Закон РБ**«Об авторском праве и смежных правах»**от 16.05.1996 (ред. 2004 г.) – Статья 6 – объектами авторского права являются БД.
2. «Концепция формирования национальной безопасности», 2006 г. – Глава VII (Обеспечение информационной безопасности). Создатели баз данных выявляют потенциальные угрозы, формируют единую политику обеспечения безопасности. Они исследуют технические и программные средства на соответствие требованиям безопасности (сертификация и лицензирование).
3. Постановление Совета Министров РБ от 12.07.2004 г. «Об утверждении государственной программы защиты информации».

Базы данных действительно отнесены действующим законодательством к числу объектов авторского права -- они упомянуты в ст. 7 Закона "Об авторском праве и смежных правах" (далее -- Закон) и ст. 993 Гражданского кодекса (ГК). Однако указание базы данных среди объектов авторского права не означает, что любая база данных автоматически, просто в силу принадлежности к категории баз данных охраняется авторским правом. В ст. 4 Закона база данных определяется как "компиляция материалов, данных, информации, по подбору и расположению материалов представляющая результат творческого труда", а согласно ст. 993 ГК "к объектам авторского права также относятся... сборники (...базы данных) и другие составные произведения, представляющие собой по подбору или расположению материалов результат творческого труда".

Таким образом, для того чтобы база данных была признана объектом авторского права, необходимо соблюдение двух условий: 1) деятельность по подбору информации, включаемой в базу данных, должна носить творческий характер, и 2) расположение информации внутри базы данных должно быть результатом творческой деятельности.

Творческая деятельность представляет собой интеллектуальную деятельность, в результате которой мысли и образы автора облекаются в определенную объективную форму, являющуюся новой, оригинальной, отличной от уже существующих объектов.

Если рассматривать справочную базу данных некоторого предприятия связи с точки зрения соответствия критерию творчества, то можно прийти к следующим выводам. Во-первых, база данных предприятия связи не является результатом творческой деятельности по подбору информации, поскольку включает в себя информацию обо всех абонентах, обслуживаемых этим предприятием; подбор информации для включения в базу попросту не осуществляется -- в базу заносится информация о каждом, кто становится абонентом. Во-вторых, внутри базы данных информация расположена стандартным образом (по номерам и алфавиту); какой-либо оригинальности в расположении информации в базе данных предприятия "Брестоблтелеком", отличающей ее от аналогичных баз данных других областных предприятий связи, нет. Поэтому справочная база данных телефонных номеров УП "Брестоблтелеком", не являясь по подбору и расположению включенной в нее информации результатом творческой деятельности, не может являться объектом авторского права. А поскольку эта база данных объектом авторского права не является, то и претензии, связанные с якобы имевшим место нарушением авторских прав, также безосновательны.

Более того, особенность правовой охраны базы данных как составного произведения состоит в том, что предметом охраны являются именно оригинальные подборка и расположение информации в базе данных, но не сама информация: "Охрана не распространяется непосредственно на сами данные..." -- (ст. 7 Закона). В соответствии с п.2 ст.8 Закона авторское право не распространяется на информацию, даже если она воплощена в охраняемом авторским правом произведении. Говорить же о правовой охране собственно информации из справочной базы данных предприятия связи также не приходится, поскольку эта информация не отвечает требованиям, установленным в ст.140 ГК, и поэтому не относится к категории охраняемой.

Конфликт, возникший между издателем телефонного справочника и предприятием связи, напоминает те споры, которое не так давно возникали между телерадиокомпаниями и печатными СМИ из-за программ теле- и радиопередач. Первые настаивали на том, что газеты и журналы, публикуя эти программы, нарушают авторское право телерадиокомпаний, вторые говорили о том, что такие программы объектом авторского права не являются. Наиболее остро эти споры проходили в Российской Федерации, где в судах было рассмотрено значительное число исков телерадиокомпаний. В большинстве случаев в исках было отказано: суды не признавали программу передач объектом авторского права именно в силу отсутствия творчества при ее создании.

Безусловно, все сказанное не означает, что ситуация, при которой один субъект хозяйствования вкладывает силы и средства в создание информационного ресурса, а другой субъект несанкционированно пользуется результатами его труда, является правильной. Вовсе нет. Вопросы правовой охраны так называемых "инвестиционных" баз данных - информационных ресурсов, создание которых требует значительных средств, но которые при этом являются неохраноспособными с точки зрения авторского права, являются весьма актуальными. В развитых странах принимаются законодательные акты, предоставляющие специальную правовую охрану подобным базам данных. Однако в Беларуси эта проблема пока даже не обсуждается. Поэтому вывод может быть один: решать конфликтную ситуацию следует в соответствии с тем законодательством, которое действует. А оно не дает оснований белорусским предприятиям связи претендовать на обладание авторским правом ни на телефонные справочники, ни на монопольное владение информацией из них (*Сергей ЛОСЕВ, кандидат юридических наук)*.

https://studfiles.net/html/2706/1067/html_wK6mevxKd_.zBh9/img-YGsiXt.pnghttps://studfiles.net/html/2706/1067/html_wK6mevxKd_.zBh9/img-oov4kc.pngИмущественные права на программу для ЭВМ или БД, созданную в порядке выполнения служебных обязанностей или по заданию работодателя, принадлежат работодателю, если в договоре между ним и автором не предусмотрено иное. Правовые отношения между работодателем и разработчиком программы для ЭВМ и БД должны регулироваться "Дополнительным соглашением к трудовому договору (контракту) по вопросам интеллектуальной собственности" или "Авторским договором о передаче прав на использование произведений, созданных в порядке выполнения служебного задания". За автором сохраняются только личные неимущественные права. При этом порядок выплаты и размер вознаграждения также устанавливаются договором.

Целесообразность заключения договора (контракта) для работодателя определяется следующими преимуществами:

Во-первых, заключение такого договора может лишить работника оснований (прежде всего экономических) искать пути передачи созданной им разработки третьим лицам без уведомления об этом работодателя. На практике это обеспечивается включением в договор условий о выплате автору в качестве вознаграждения определенного процента с дохода (прибыли), полученного работодателем от реализации его разработки, дополнительно к заработной плате.

Во-вторых, это гарантирует работодателю выполнение всех обязательств перед заказчиками, покупателями, пользователями и иными лицами в части сопровождения программ для ЭВМ, доступности исходного кода, последующих модификаций и усовершенствований и т.п. Эти вопросы также могут быть оговорены в договоре с работником.

В-третьих, появляется дополнительная возможность стимулировать работника к созданию оригинальной конкурентоспособной разработки. Разработчик лично заинтересован в её дальнейшей реализации работодателем при уверенности в том, что с каждой продажи третьим лицам он будет получать справедливое вознаграждение.

В-четвертых, соблюдение работником условий конфиденциальности в отношении информации, затрагивающей интересы работодателя и ставшей ему доступной в процессе работы по заданию работодателя, также может быть отражено в таком договоре

Работник, как правило, тоже бывает заинтересован в заключении подобного договора, не содержащего кабальных для него условий, а, наоборот, предусматривающего выплату вознаграждения с четким указанием его размеров и сроков получения.

И, наконец, автор может создавать программу для ЭВМ или БД по заказу другого физического или юридического лица. В этом случае между автором и заказчиком изначально должен быть заключен авторский договор заказа на создание и передачу программы для ЭВМ или БД. Согласно этому договору автор обязуется создать и передать заказанную программу или БД в соответствии с условиями договора, а заказчик обязан в счет установленного в договоре вознаграждения выплатить автору аванс. При этом по условиям авторского договора автор может передать заказчику имущественные права полностью или частично.