Лекция 8. "Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом"

Литература

- В.А. Галатенко «Основы информационной безопасности», Электронная книга

Основные понятия программно-технического уровня информационной безопасности

Центральным для программно-технического уровня является понятие **сервиса безопасности**.

Основные понятия программно-технического уровня информационной безопасности

К вспомогательным относятся сервисы безопасности (мы уже сталкивались с ними при рассмотрении стандартов и спецификаций в области ИБ); среди них нас в первую очередь будут интересовать универсальные, высокоуровневые, допускающие использование различными **основными и вспомогательными сервисами** .

Основные понятия программно-технического уровня информационной безопасности

Далее мы рассмотрим следующие сервисы:

- идентификация и аутентификация ;
- управление доступом ;
- протоколирование и аудит ;
- шифрование ;
- контроль целостности ;
- экранирование ;
- анализ защищенности ;
- обеспечение отказоустойчивости ;
- обеспечение безопасного восстановления ;
- туннелирование ;
- управление.

Основные понятия программно-технического уровня информационной безопасности

Для проведения классификации сервисов безопасности и определения их места в общей архитектуре меры безопасности можно разделить на следующие виды:

- превентивные, препятствующие нарушениям ИБ;
- меры обнаружения нарушений ;
- локализующие, сужающие зону воздействия нарушений;
- меры по выявлению нарушителя ;
- меры восстановления режима безопасности.

Основные понятия программно-технического уровня информационной безопасности

Большинство сервисов безопасности попадает в число превентивных, и это, безусловно, правильно. Аудит и контроль целостности способны помочь в обнаружении нарушений ; активный аудит, кроме того, позволяет запрограммировать реакцию на нарушение с целью локализации и/или прослеживания. Направленность сервисов отказоустойчивости и безопасного восстановления очевидна. Наконец, управление играет инфраструктурную роль, обслуживая все аспекты ИС.

Идентификация и аутентификация

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя).

Идентификация и аутентификация

Посредством **аутентификации** вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова " аутентификация " иногда используют словосочетание "проверка подлинности".

Аутентификация

Аутентификация — процедура проверки подлинности, например:

- проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей;
- подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;
- проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Авторизация

Авторизация— предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

Часто можно услышать выражение, что какой-то человек «авторизован» для выполнения данной операции — это значит, что он имеет на неё право.

Авторизация

Авторизацию не следует путать с аутентификацией: аутентификация — это процедура проверки легальности пользователя или данных, например, проверки соответствия введённого пользователем пароля к учётной записи паролю в базе данных, или проверка цифровой подписи письма по ключу шифрования, или проверка контрольной суммы файла на соответствие заявленной автором этого файла.

Авторизация же производит контроль доступа легальных пользователей к ресурсам системы после успешного прохождения ими аутентификации. Зачастую процедуры аутентификации и авторизации совмещаются.

Идентификация и аутентификация

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.

Парольная аутентификация

Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Парольная аутентификация

Следующие меры позволяют значительно повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");
- обучение пользователей;
- использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Одноразовые пароли

Рассмотренные выше **пароли можно назвать многоразовыми** ; их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются **одноразовые пароли**.

Сервер аутентификации Kerberos

Kerberos – это программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

Идентификация/аутентификация с помощью биометрических данных

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности **отпечатков пальцев**, **сетчатки** и **роговицы** глаз, **геометрия руки и лица** и т.п. К поведенческим характеристикам относятся **динамика подписи** (ручной), стиль **работы с клавиатурой**. На стыке физиологии и поведения находятся анализ особенностей **голоса** и **распознавание речи**.

Идентификация/аутентификация с помощью биометрических данных

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый **биометрическим шаблоном**) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

Идентификация/аутентификация с помощью биометрических данных

Но главная опасность состоит в том, что любая "пробоина" для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей системы.

Модели управления доступом

Цели и область применения

Цель управления доступом это ограничение операций которые может проводить легитимный пользователь (зарегистрировавшийся в системе). Управление доступом указывает что конкретно пользователь имеет право делать в системе, а так же какие операции разрешены для выполнения приложениями, выступающими от имени пользователя.

Цели и область применения

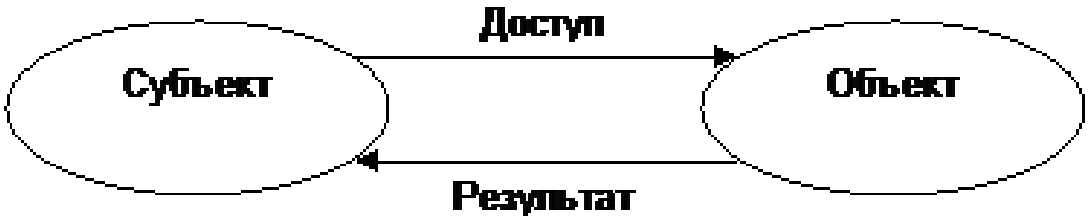
Таким образом управление доступом предназначено для предотвращения действий пользователя, которые могут нанести вред системе, например нарушить безопасность системы.

Используемые термины

Доступ	Доступ субъекта к объекту для определенных операций.
Объект	Контейнер информации в системе
Субъект	Сущность определяющая пользователя при работе в системе
Пользователь	Человек выполняющий действия в системе или приложение выступающее от его имени.

Общее описание

Управление доступом это определение возможности субъекта оперировать над объектом. В общем виде описывается следующей диаграммой:



Общее описание

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над **объектами** (информацией и другими компьютерными ресурсами). В данном разделе речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Общее описание

Задача: обеспечить управление доступом к производственной информации.

Доступ к компьютерным системам и данным необходимо контролировать исходя из производственных требований (бизнеса).

Такой контроль должен учитывать правила распространения информации и разграничения доступа, принятые в организации.

Общее описание

Производственные требования к управлению доступом к системам необходимо определить и документально оформить.

Правила управления доступом и права доступа для каждого пользователя или группы пользователей должны быть четко сформулированы в положениях политики управления доступом к информации. Пользователи и поставщики услуг должны знать четко сформулированные производственные требования, удовлетворяющие политике управления доступом.

Общее описание

При определении правил управления доступом необходимо рассмотреть следующее:

- различия между правилами, которые всегда должны быть выполнены, и правилами, которые являются необязательными или условными;
- формулировать правила лучше на предпосылке "запрещено все, что явно не разрешено", чем на предпосылке "разрешено все, что явно не запрещено";
- изменения в информационных метках, которые инициализированы автоматически средствами обработки информации и инициализированы по усмотрению пользователя;
- изменения в правах доступа пользователю, которые инициализированы автоматически информационной системой и инициализированы администратором;
- правила, которые требуют одобрения администратора или кого-либо другого перед вступлением в силу, и те правила, которые не требуют чьего-либо одобрения.

Модели управления доступом

- Избирательное управление доступом
- Полномочное управление доступом
- Ролевое управление доступом

Избирательное управление доступом

Избирательное управление доступом (англ. *discretionary access control*, DAC) — управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа.

Также используются названия *«дискреционное управление доступом»*, *«контролируемое управление доступом»* или *«разграничительное управление доступом»*.

Избирательное управление доступом

- Каждый объект системы имеет привязанного к нему субъекта, называемого **владельцем**. Именно владелец устанавливает права доступа к объекту.
- Система имеет одного выделенного субъекта — суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.
- Субъект с определенным правом доступа может передать это право любому другому субъектуп
- Права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе **матрицы доступа** (МД, иногда ее называют матрицей контроля доступа). Такая модель получила название матричной.

Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту - столбец. На пересечении столбца и строки матрицы указывается тип (типы) разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту как "доступ на чтение", "доступ на запись", "доступ на исполнение" и др.

Избирательное управление доступом

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе.

Например, доступ субъекта к конкретному объекту может быть разрешен только в определенные дни (дата-зависимое условие), часы (время-зависимое условие), в зависимости от других характеристик субъекта (контекстно-зависимое условие) или в зависимости от характера предыдущей работы. Такие условия на доступ к объектам обычно используются в СУБД. Кроме того, субъект с определенными полномочиями может передать их другому субъекту (если это не противоречит правилам политики безопасности).

Решение на доступ субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно, избирательное управление доступом реализует принцип "что не разрешено, то запрещено", предполагающий явное разрешение доступа субъекта к объекту.

Избирательное управление доступом

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и/или изменения его владельца. Именно такой смешанный вариант реализован в большинстве операционных систем, например Unix или Windows NT.

Полномочное управление доступом

Мандатное управление доступом (англ. *Mandatory access control, MAC*) — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

Также иногда переводится как **Принудительный контроль доступа**. Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования.

Полномочное управление доступом

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;
- каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Полномочное управление доступом

В том случае, когда совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру и, таким образом, в системе можно реализовать иерархически не нисходящий (по ценности) поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности.

Каждый субъект кроме уровня прозрачности имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности. Для принятия решения на разрешение доступа производится сравнение метки критичности объекта с уровнем прозрачности и текущим уровнем безопасности субъекта.

Полномочное управление доступом

Результат сравнения определяется двумя правилами: простым условием защиты (simple security condition) и свойством (property). В упрощенном виде, они определяют, что информация может передаваться только "наверх", то есть субъект может читать содержимое объекта, если его текущий уровень безопасности не ниже метки критичности объекта, и записывать в него, если не выше.

Простое условие защиты гласит, что любую операцию над объектом субъект может выполнять только в том случае, если его уровень прозрачности не ниже метки критичности объекта.

Полномочное управление доступом

Основное назначение полномочной политики безопасности - регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Мандатная система разграничения доступа реализована в ОС FreeBSD Unix.

В SUSE Linux и Ubuntu есть архитектура мандатного контроля доступа под названием AppArmor.

Ролевое управление доступом

Управление доступом на основе ролей (англ. *Role Based Access Control, RBAC*) — развитие политики избирательного управления доступом, при этом права доступа субъектов системы на объекты группируются с учётом специфики их применения, образуя роли.

Ролевое управление доступом

Ролевая модель управления доступом содержит ряд особенностей, которые не позволяют отнести её ни к категории дискреционных, ни к категории мандатных моделей.

Основная идея реализуемого в данной модели подхода состоит в том, что понятие «субъект» заменяется двумя новыми понятиями:

- пользователь – человек, работающий в системе;
- роль – активно действующая в системе абстрактная сущность, с которой связан ограниченный и логически непротиворечивый набор полномочий, необходимых для осуществления тех или иных действий в системе.

Ролевое управление доступом

Классическим примером роли является root в Unix-подобных системах – суперпользователь, обладающий неограниченными полномочиями. Данная роль по мере необходимости может быть задействована различными администраторами.

Основным достоинством ролевой модели является близость к реальной жизни: роли, действующие в АС, могут быть выстроены в полном соответствии с корпоративной иерархией и при этом привязаны не к конкретным пользователям, а к должностям – что, в частности, упрощает администрирование в условиях большой текучки кадров.

Ролевое управление доступом

Управление доступом при использовании ролевой модели осуществляется следующим образом:

1. Для каждой роли указывается набор полномочий, представляющий собой набор прав доступа к объектам АС.
2. Каждому пользователю назначается список доступных ему ролей.

Отметим, что пользователь может быть ассоциирован с несколькими ролями – данная возможность также значительно упрощает администрирование сложных корпоративных АС.

Ролевое управление доступом

RBAC широко используется для управления пользовательскими привилегиями в пределах единой системы или приложения. Список таких систем включает в себя Microsoft Active Directory, SELinux, FreeBSD, Solaris, СУБД Oracle и множество других.

Модель Белла — Лападулы

Модель Белла — Лападулы — модель контроля и управления доступом, основанная на мандатной модели управления доступом. В модели анализируются условия, при которых невозможно создание информационных потоков от субъектов с более высоким уровнем доступа к субъектам с более низким уровнем доступа.

Модель Белла — Лападулы

Классическая модель Белла — Лападулы была описана в 1975 году сотрудниками компании MITRE Corporation Дэвидом Беллом и Леонардом Лападулой, к созданию модели их подтолкнула система безопасности для работы с секретными документами Правительства США.

Суть системы заключалась в следующем: каждому субъекту (лицу, работающему с документами) и объекту (документам) присваивается метка конфиденциальности, начиная от самой высокой («особой важности»), заканчивая самой низкой («несекретный» или «общедоступный»). Причем субъект, которому разрешён доступ только к объектам с более низкой меткой конфиденциальности, не может получить доступ к объекту с более высокой меткой конфиденциальности. Также субъекту запрещается запись информации в объекты с более низким уровнем безопасности.

Модель Харрисона-Руззо-Ульмана

Модель Харрисона-Руззо-Ульмана является классической дискреционной моделью, реализует произвольное управление доступом субъектов к объектам и контроль за распределение прав доступа в рамках этой модели.

Модель Харрисона-Рузза-Ульмана

Система обработки предоставляется в виде совокупности активных сущностей субъектов, формирующих множество субъектов , которые осуществляют доступ к пользователям пассивных сущностей объектов , формирующих множество объектов , содержащих защищаемую информацию, и конечного множества прав доступа , характеризующего полномочия на выполнение соответствующих действий до того, что бы включить в область действия модели отношения между субъектами. Принято считать, что все субъекты одновременно являются и объектами.

Модель пятимерного пространства безопасности Хордстона

Теперь рассмотрим модель, называемую пятимерным пространством безопасности Хартстона. В данной модели используется пятимерное пространство безопасности для моделирования процессов, установления полномочий и организации доступа на их основании. Модель имеет пять основных наборов:

A – установленных полномочий; U – пользователей; E – операций; R – ресурсов; S – состояний.

Модель пятимерного пространства безопасности Хордстона

Область безопасности будет выглядеть как декартово произведение: A×U×E×R×S. Доступ рассматривается как ряд запросов, осуществляемых пользователями u для выполнения операций e над ресурсами R в то время, когда система находится в состоянии s. Например, запрос на доступ представляется четырехмерным кортежем q = (u, e, R, s), $u \in U, e \in E, s \in S, r \in R$. Величины u и s задаются системой в фиксированном виде.

Таким образом, запрос на доступ – подпространство четырехмерной проекции пространства безопасности. Запросы получают право на доступ в том случае, когда они полностью заключены в соответствующие подпространства.

Монитор безопасности обращений

Концепция монитора безопасности обращений является достаточно естественной формализацией некого механизма, реализующего разграничение доступа в системе.

Монитор безопасности обращений (МБО) представляет собой фильтр, который разрешает или запрещает доступ, основываясь на установленных в системе правилах разграничения доступа

Монитор безопасности обращений

Получив запрос на доступ от субъекта S к объекту O, монитор безопасности обращений анализирует базу правил, соответствующую установленной в системе политике безопасности, и либо разрешает, либо запрещает доступ.

Монитор безопасности обращений удовлетворяет следующим свойствам:

1. Ни один запрос на доступ субъекта к объекту не должен выполняться в обход МБО.
2. Работа МБО должна быть защищена от постороннего вмешательства.
3. Представление МБО должно быть достаточно простым для возможности верификации корректности его работы.

Несмотря на то, что концепция монитора безопасности обращений является абстракцией, перечисленные свойства справедливы и для программных или аппаратных модулей, реализующих функции монитора обращений в реальных системах.

Модели целостности

Одной из целей политики безопасности— защита от нарушения целостности информации.

Наиболее известны в этом классе моделей **модель целостности Биба** и **модель Кларка—Вильсона**.

Модель Кларка-Вилсона

Модель Кларка-Вилсона появилась в результате проведенного авторами анализа реально применяемых методов обеспечения целостности документооборота в коммерческих компаниях. В отличие от моделей Биба и Белла-ЛаПадулы, она изначально ориентирована на нужды коммерческих заказчиков, и, по мнению авторов, более адекватна их требованиям, чем предложенная ранее коммерческая интерпретация модели целостности на основе решеток.

Модель Кларка-Вилсона

Основные понятия рассматриваемой модели — это корректность транзакций и разграничение функциональных обязанностей. Модель задает правила функционирования компьютерной системы и определяет две категории объектов данных и два класса операций над ними. Все содержащиеся в системе данные подразделяются на контролируемые и неконтролируемые элементы данных (constrained data items — CDI и unconstrained data items — UDI соответственно). Целостность первых обеспечивается моделью Кларка-Вилсона. Последние содержат информацию, целостность которой в рамках данной модели не контролируется (этим и объясняется выбор терминологии).

Модель Кларка-Вилсона

Далее, модель вводит два класса операций над элементами данных: процедуры контроля целостности (integrity verification procedures — IVP) и процедуры преобразования (transformation procedures — TP). Первые из них обеспечивают проверку целостности контролируемых элементов данных (CDI), вторые изменяют состав множества всех CDI (например, преобразуя элементы UDI в CDI).

Модель Кларка-Вилсона

Так же модель содержит девять правил, определяющих взаимоотношения элементов данных и процедур в процессе функционирования системы.

- Правило C1. Множество всех процедур контроля целостности (IVP) должно содержать процедуры контроля целостности любого элемента данных из множества всех CDI.
- Правило C2. Все процедуры преобразования (TP) должны быть реализованы корректно в том смысле, что не должны нарушать целостность обрабатываемых ими CDI. Кроме того, с каждой процедурой преобразования должен быть связан список элементов CDI, которые допустимо обрабатывать данной процедурой. Такая связь устанавливается администратором безопасности.
- Правило E1. Система должна контролировать допустимость применения TP к элементам CDI в соответствии со списками, указанными в правиле C2.
- Правило E2. Система должна поддерживать список разрешенных конкретным пользователям процедур преобразования с указанием допустимого для каждой TP и данного пользователя набора обрабатываемых элементов CDI.
- Правило C3. Список, определенный правилом C2, должен отвечать требованию разграничения функциональных обязанностей.
- Правило E3. Система должна аутентифицировать всех пользователей, пытающихся выполнить какую-либо процедуру преобразования.
- Правило C4. Каждая TP должна записывать в журнал регистрации информацию, достаточную для восстановления полной картины каждого применения этой TP. Журнал регистрации — это специальный элемент CDI, предназначенный только для добавления в него информации.
- Правило C5. Любая TP, которая обрабатывает элемент UDI, должна выполнять только корректные преобразования этого элемента, в результате которых UDI превращается в CDI.
- Правило E4. Только специально уполномоченное лицо может изменять списки, определенные в правилах C2 и E2. Это лицо не имеет права выполнять какие-либо действия, если оно уполномочено изменять регламентирующие эти действия списки.

Модель Биба

В основе модели Биба лежат уровни целостности, аналогичные уровням модели Белла—Лападула. В отличие от модели Белла—Лападула чтение разрешено теперь только вверх (от субъекта к объекту, уровень ценности которого превосходит уровня субъекта), а запись — только вниз. Правила данной модели являются полной противоположностью правилам модели Белла—Лападула.

Модель Биба

В модели Биба рассматриваются следующие доступы субъектов к объектам и другим субъектам: доступ субъекта на модификацию объекта, доступ субъекта на чтение объекта, доступ субъекта на выполнение и доступ субъекта к субъекту.

Модель Биба

Отдельного комментария заслуживает вопрос, что именно понимается в модели Биба под уровнями целостности.

Действительно, в большинстве приложений целостность данных рассматривается как некое свойство, которое либо сохраняется, либо не сохраняется – и введение иерархических уровней целостности может представляться излишним.

В действительности уровни целостности в модели Биба стоит рассматривать как уровни достоверности, а соответствующие информационные потоки – как передачу информации из более достоверной совокупности данных в менее достоверную и наоборот.