# Тема 5

Управление доступом к информации в базах данных

# Содержание темы

- Классификация компонент доступа, правила разграничения доступа к информации в базах данных.
- Принципы построения системы разграничения доступа к информации в базах данных.
- Механизмы управления доступом к информации в базах данных.
- Алгоритмы управления доступом к базах данных.
- Закон Республики Беларусь № 170-З «О государственных секретах» от 19 июля 2010 г.

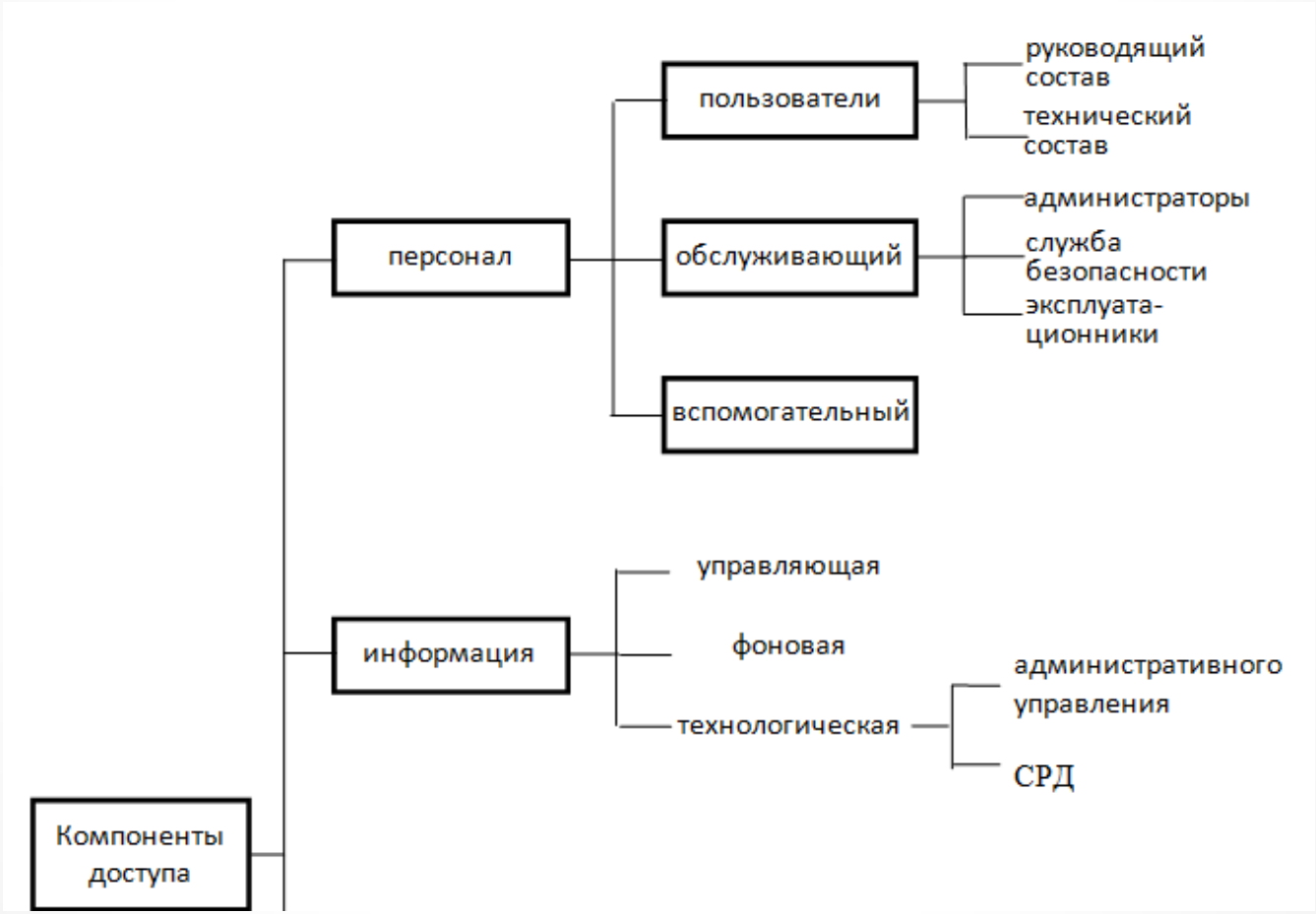
# Авторизация субъектов

**Авторизация** - это процедура контроля доступа легальных субъектов к ресурсам системы и предоставление каждому из них именно тех прав, которые ему были определены администратором.

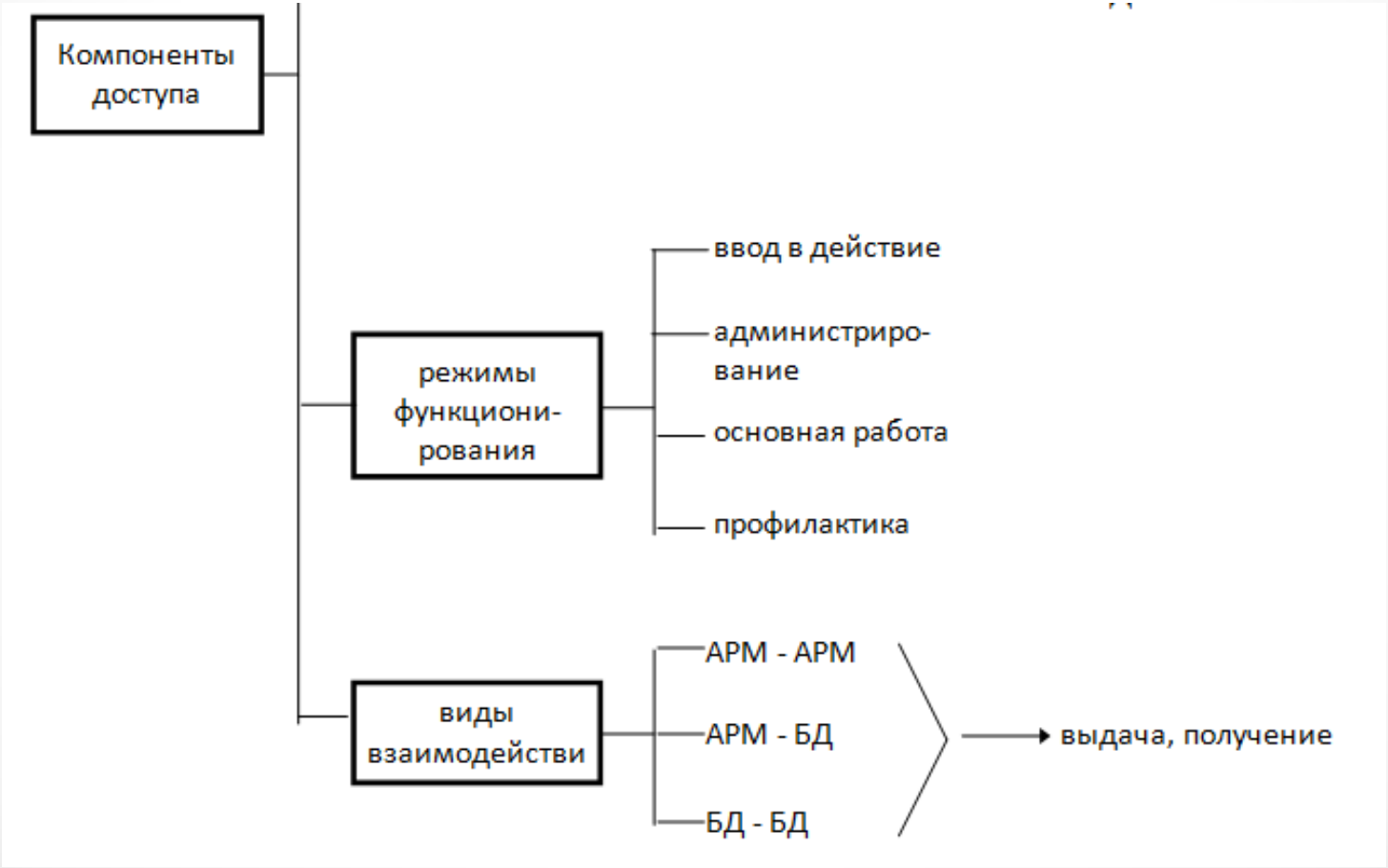
Термин **авторизация** (authorization) происходит от латинского слова auctoritas, показывающее уровень престижа человека в Древнем Риме и соответствующие этому уровню привилегии.

Помимо предоставления пользователям прав доступа к каталогам, файлам и принтерам, средства авторизации могут контролировать возможность выполнения пользователями различных системных функций.

# Классификация компонент доступа



# Классификация компонент доступа



# Принципы построения ПРД

Ограничение доступа может задаваться в форме **правил**.

На основании правил система управления доступом в любой момент времени динамически решает вопрос о предоставлении или не предоставлении доступа.

Правило строится с учетом различных факторов, например:

- длительность сеанса связи;
- возраст;
- время суток и т. п.

# Принципы построения ПРД

**Правила разграничения доступа** (**ПРД**) основываются на следующих принципах:

1) субъектам должны быть представлены все необходимые ресурсы системы для выполнения ими своих функциональных обязанностей;

2) ПРД не должны нарушать функциональные связи субъектов в сложившейся структуре управления;

3) ПРД должны отражать требования соблюдения режима секретности и сохранения государственной и коммерческой тайны при обработке информации в ТКС;

# Принципы построения ПРД

4) действия субъектов с информацией, не оговоренные ПРД, должны быть запрещены;

5) субъектам должен быть разрешен доступ только к той информации, которая необходима им в настоящее время для выполнения своих функций.

# Принципы построения ПРД

Взаимодействие субъектов с объектами обозначается

$$(s, a) \in S \times A = D$$

и называется доступом субъекта $s$ к объекту $a$.

П – это правила разграничения доступа, по которым каждому объекту и субъекту ставится в соответствие определенный доступ.

Задать правила П по существу означает определить подмножество

$$П \subset S \times A$$

разрешенных доступов.

# Принципы построения ПРД

Функционирование информационной системы с точки зрения защиты можно рассматривать как последовательность реализаций во времени определенной совокупности связей между множествами $S$ и $A$.

Множество $T = \{t\}$ моментов времени, в которые рассматривается функционирование системы.

$R$ - множество доступов, которые имели место

$$R \subset S \times A.$$

# Принципы построения ПРД

С точки зрения защиты, на пространстве функциональных состояний системы, определяемых решаемыми задачами управления и обработки данных, можно выделить четыре группы состояний, которые обозначим $Ф_i(t)$.

# Принципы построения ПРД

К первой группе относится множество состояний, в которых был реализован доступ, не противоречащий правилам П.

$$Ф_1 = П \cap R.$$

Множество состояний $Ф_1$ системы, характеризующихся тем, что реализуется доступ только разрешенный правилами П, называются безопасными состояниями.

# Принципы построения ПРД

Ко второй группе относится множество состояний нереализованных доступов, которые запрещены правилами П.

$$\Phi_2 = \overline{\Pi} \cap \overline{R}$$

Множества $\overline{\Pi} \cap \overline{R}$ являются дополнением множеств П и *R* к множеству *D*. Множество $\Phi_2$ отражает состояние системы, в которые она переходит при воздействии на нее факторов внешней среды.

# Принципы построения ПРД

Третью группу составляет множество состояний реализованных доступов, которые запрещены правилами

$$\Phi_3 = \overline{\Pi} \cap R.$$

Нахождение системы на множестве состояний $\Phi_3$ характеризует тот факт, что система полностью не смогла защититься от воздействия факторов внешней среды и доступ субъектов в нарушение правил П имел место.

Доступ в состоянии $\Phi_3$ является **несанкционированным доступом** (**НСД**).

# Принципы построения ПРД

Четвертую группу составляет множество состояний нереализованных доступов, которые разрешены правилами

$$\Phi_4 = \Pi \cap \overline{R}.$$

Множество $\Phi_4$ состояний определяется тем, что в силу случайности множества  защита может вызвать блокировку доступа (*s*, *a*), необходимого для функционирования системы, вследствие перегрузки или сбоя.

# Принципы построения ПРД

Разграничение доступа в общем случае предполагает реализацию **системы разграничения доступа** (**СРД**), обеспечивающую реализацию разрешенного доступа и блокирующую доступ запрещенный.

Должна быть создана подсистема, работа которой должна сводиться к определению принадлежности пары (*s*, *a*) к П и блокировке ее реализации в условиях, что системе может быть навязана ложная информация о принадлежности к П.

# Механизмы управления доступом к инф. в БД

Разграничение доступа может осуществляться несколькими способами:

- По **спискам контроля доступа** (**ACL – Access Control List**);
- С использованием **избирательного** или **дискреционного управления доступом** (**DAC – Discretionary Access Control**, матрицей контроля доступа);
- С помощью **полномочного** или **мандатного управления доступом** (**MAC – Mandatory Access Control**) – по уровням секретности;
- По **ролевому доступу** (**RBAC – Role-based Access Control**) – недискреционному методу доступа.

# Механизмы управления доступом к инф. в БД

Разграничение доступа по **спискам контроля доступа** заключается в том, что для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа.

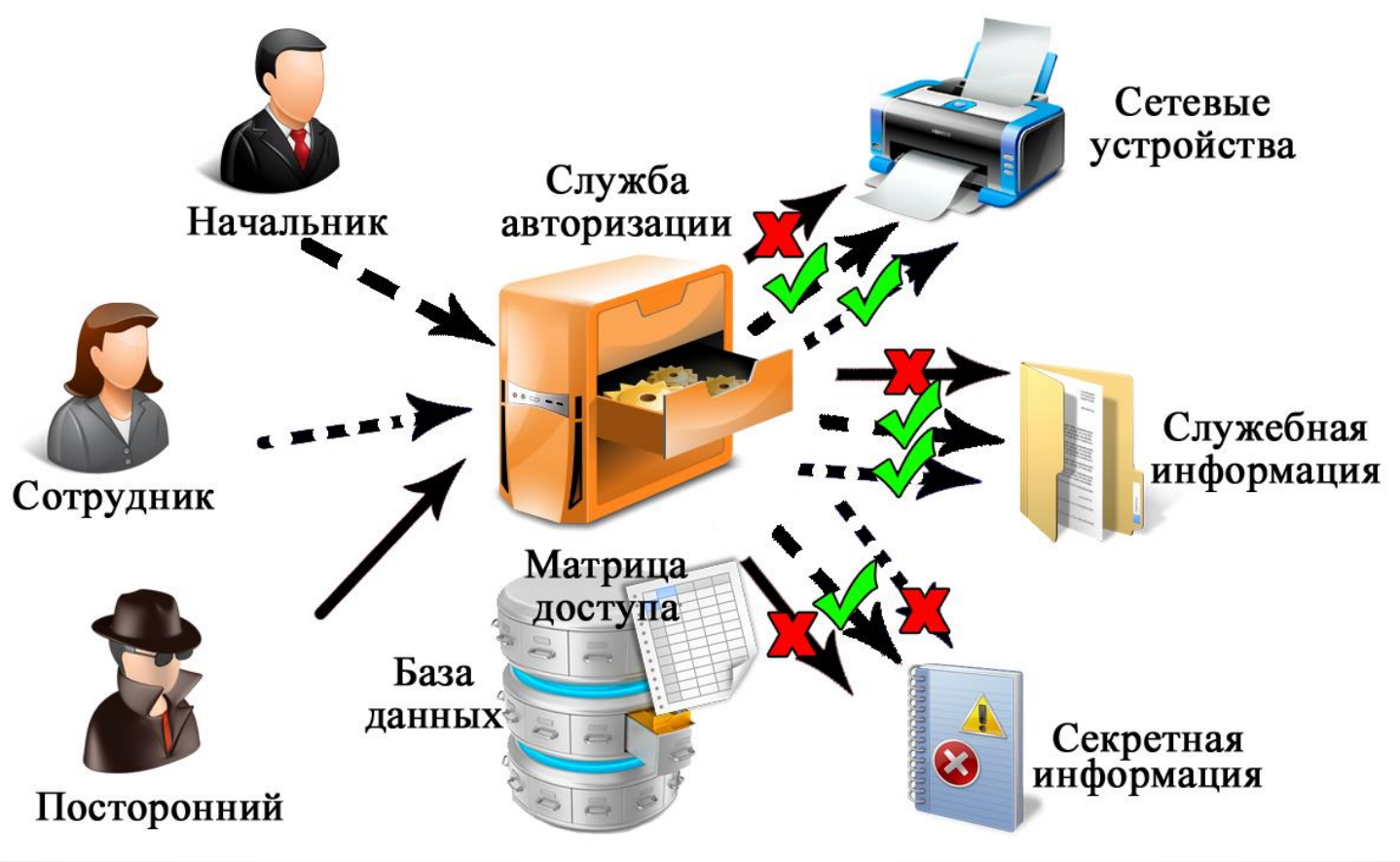
# Механизмы управления доступом к инф. в БД

**Избирательное** или **дискреционное управление доступом** (разграничение доступа по матрицам полномочий) предполагает формирование двумерной матрицы, по строкам которой содержатся идентификаторы зарегистрированных пользователей, а по столбцам – идентификаторы защищаемых элементов данных (*X* – нет прав; *R* – чтение; *W* – запись; *C* – создание; *E* – редактирование; *D* – удаление).

| Субъект | Объект | | | |
|---|---|---|---|---|
| | персональные данные сотрудника | финансовый отчет | методическое пособие | приказ |
| **Ректор** | R | R | R | R, W, C, D |
| **Главный бухгалтер** | R | W, C, E | R | R |
| **Преподаватель** | X | X | W, R, C, E, D | R |
| **Студент** | X | X | R | R |

# Механизмы управления доступом к инф. в БД

Схема реализации дискреционного управления доступом

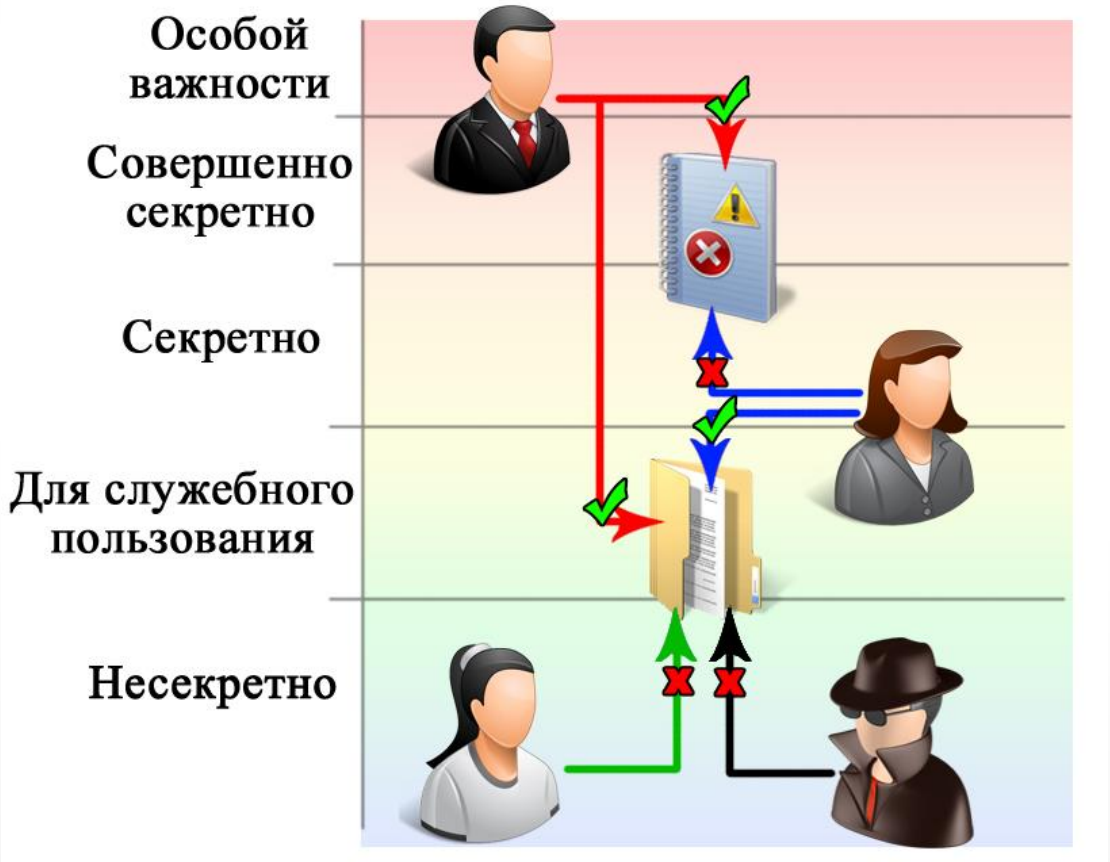


# Механизмы управления доступом к инф. в БД

**Полномочное** (**мандатное**) **управление доступом** есть способ разового разрешения на допуск к защищаемому элементу данных. Заключается он в том, что каждому защищаемому элементу присваивается персональная уникальная метка, после чего доступ к этому элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владелец элемента.

# Механизмы управления доступом к инф. в БД

Схема реализации мандатного управления доступом



# Механизмы управления доступом к инф. в БД

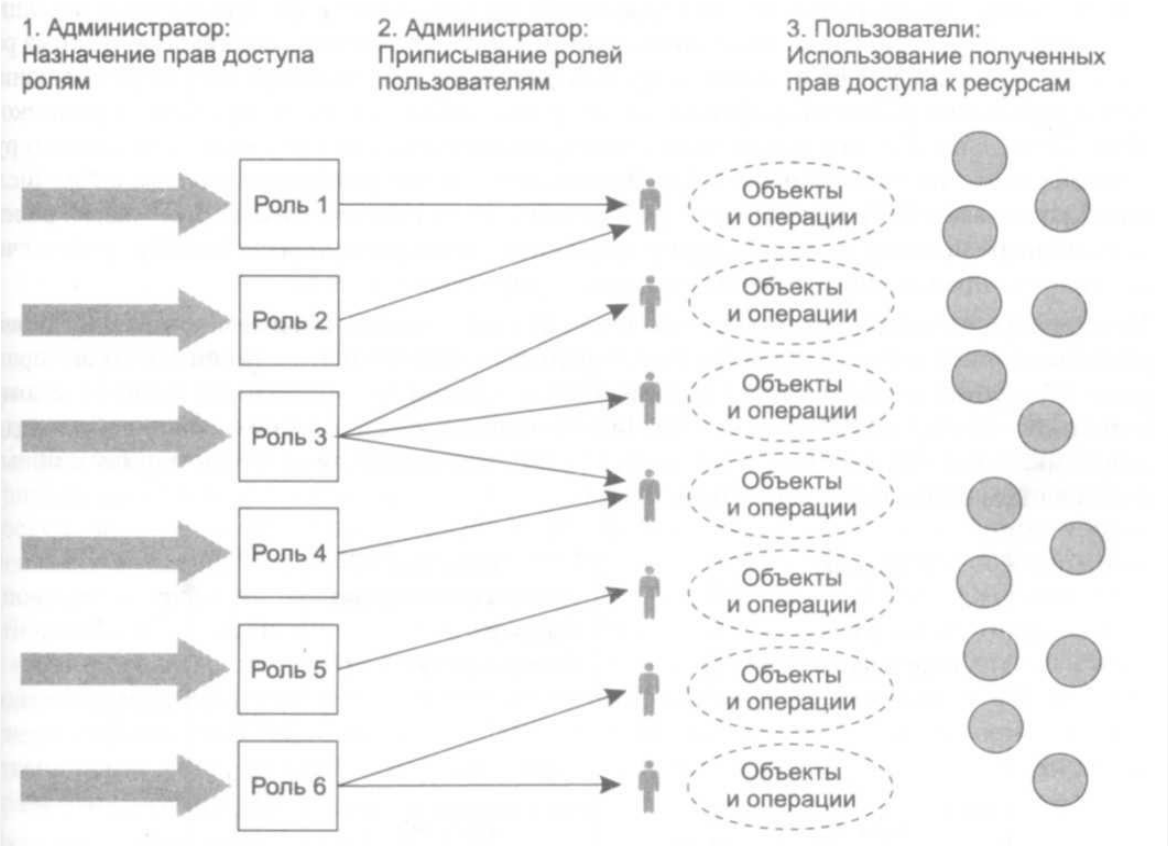
**Ролевое управление доступом** использует роли, которые по сути соответствуют понятиям «должность» и «круг должностных обязанностей».

Набор ролей должен соответствовать перечню различных должностей , существующих на предприятии.

Одна и та же роль может быть приписана разным субъектам.

# Механизмы управления доступом к инф. в БД

Схема авторизации в системах управления доступом на основе ролей



# Алгоритм управления доступом к БД

*S* – субъекты защиты;

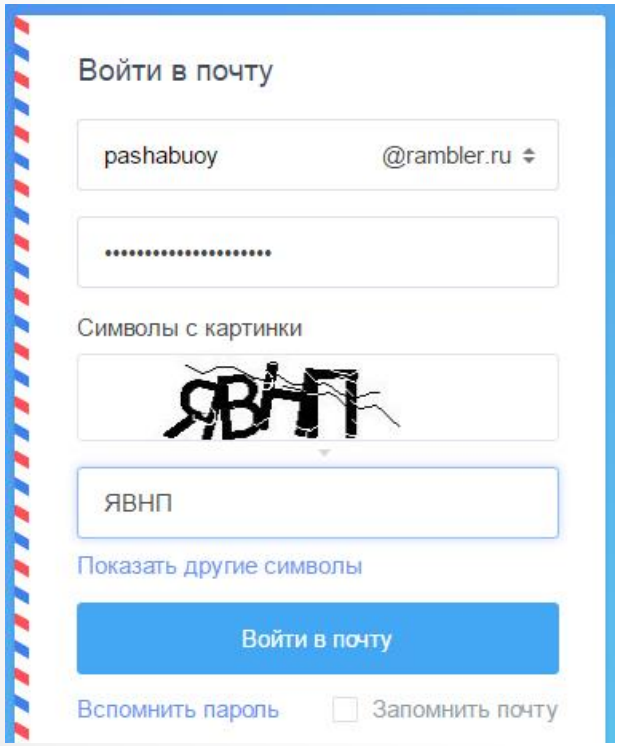
*O* – объекты защиты;

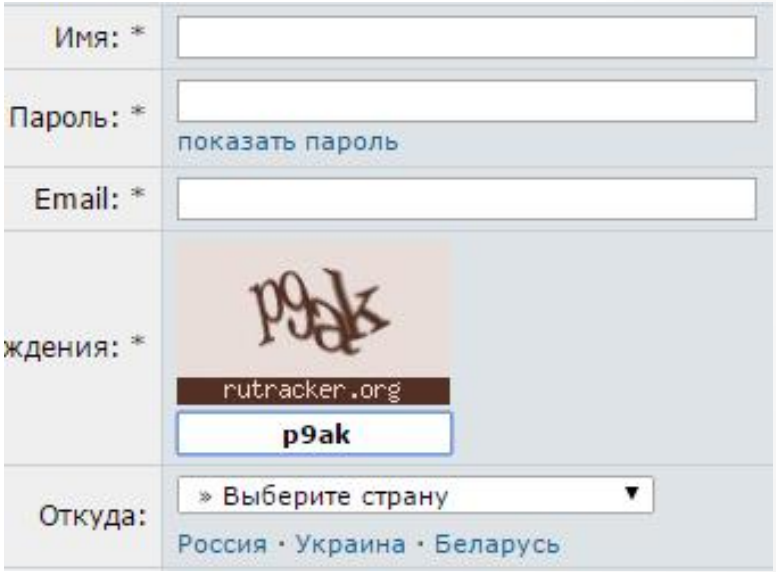
*T* – множество типов доступа;

*R* – множество полномочий доступа.

# Применение методов разграничения доступа

Популярной мерой ограничения доступа в сеть Интернет является **капча** (**Capcher**).



# Применение методов разграничения доступа

Пример дискреционного управления доступом на железнодорожной станции Ипуть БелЖД

| Действия субъектов согласно ПРД | Субъекты информационной системы | | | | | |
|---|---|---|---|---|---|---|
| | начальник станции | дежурный по станции | начальник участка СЦБ | старший электромеханик | электромеханик | диспетчер отделения дороги |
| Получение информации о поездной обстановке на станции | + | + | + | + | + | + |
| Получение специальной технологической информации по станции | + | + | – | – | – | – |
| Получение диагностической информации о системе ПРЦ по фиксированным запросам | – | – | + | + | + | – |
| Управление объектами станции с обеспечением условий безопасности движения поездов | + | + | – | – | – | – |
| Техническое обслуживание объектов управления на станции | – | – | + | + | + | – |
| Обслуживание технических средств ПРЦ | – | – | + | + | + | – |

# «О государственных секретах»

Настоящий Закон определяет правовые и организационные основы отнесения сведений к государственным секретам, защиты государственных секретов, осуществления иной деятельности в сфере государственных секретов в целях обеспечения национальной безопасности Республики Беларусь.

# «О государственных секретах»

Структура закона:

- Глава 5. Категории государственных секретов. Степени секретности. Грифы секретности;
- Глава 6. Отнесение сведений к государственным секретам. Засекречивание. Рассекречивание;
- Глава 9. Допуск к государственным секретам. Доступ к государственным секретам

# «О государственных секретах»

**Глава 5. Категории государственных секретов. Степени секретности. Грифы секретности**

**Статья 16.** Категории государственных секретов.

Государственные секреты подразделяются на две категории:

- государственная тайна (сведения, составляющие государственную тайну);
- служебная тайна (сведения, составляющие служебную тайну).

# «О государственных секретах»

**Государственная тайна** – сведения, в результате разглашения или утраты которых могут наступить тяжкие последствия для национальной безопасности Республики Беларусь.

**Служебная тайна** – сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности Республики Беларусь.

Служебная тайна может являться составной частью государственной тайны, не раскрывая ее в целом.

# «О государственных секретах»

**Статья 17.** Степени секретности.

Для государственных секретов в зависимости от тяжести последствий, которые наступили или могут наступить, размера вреда, который причинен или может быть причинен в результате их разглашения или утраты, устанавливаются следующие степени секретности:

- для государственной тайны – «Особой важности», «Совершенно секретно»;
- для служебной тайны – «Секретно».

# «О государственных секретах»

**Статья 18.** Грифы секретности.

На носителях государственных секретов и (или) сопроводительной документации к ним в зависимости от степени секретности государственных секретов проставляются следующие грифы секретности:

- на носителях государственной тайны и (или) сопроводительной документации к ним – «Особой важности», «Совершенно секретно»;
- на носителях служебной тайны и (или) сопроводительной документации к ним – «Секретно».

# «О государственных секретах»

**Глава 6. Отнесение сведений к государственным секретам. Засекречивание. Рассекречивание**

**Статья 22.** Срок засекречивания, изменение срока засекречивания.

Для государственных секретов, как правило, устанавливаются следующие сроки засекречивания:

- для государственной тайны – до тридцати лет;
- для служебной тайны – до десяти лет.

Срок засекречивания исчисляется с даты засекречивания.

# «О государственных секретах»

**Глава 9. Допуск к государственным секретам. доступ к государственным секретам**

**Статья 33.** Условия предоставления гражданам допуска к государственным секретам.

Допуск к государственным секретам гражданам предоставляется помимо прочего, если:

- имеется письменное согласие граждан на проведение в отношении их проверочных мероприятий в связи с предоставлением им допуска к государственным секретам;
- проведены проверочные мероприятия в отношении граждан в связи с предоставлением им допуска к государственным секретам.

# «О государственных секретах»

**Статья 36.** Формы допуска к государственным секретам.

В зависимости от степени секретности устанавливаются три формы допуска к государственным секретам:

- **форма № 1** – форма допуска к государственной тайне, имеющей степень секретности «Особой важности»;
- **форма № 2** – форма допуска к государственной тайне, имеющей степень секретности «Совершенно секретно»;
- **форма № 3** – форма допуска к служебной тайне, имеющей степень секретности «Секретно».