

Тема 3

Правила разграничения доступа

Содержание темы

- Авторизация субъектов.
- Основные принципы организации разграничения доступа.
- Применение методов разграничения доступа.
- Закон Республики Беларусь № 170-3 «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.

Принципы организации разграничения доступа

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 организации разграничения доступа

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.

Принципы организации разграничения доступа

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.

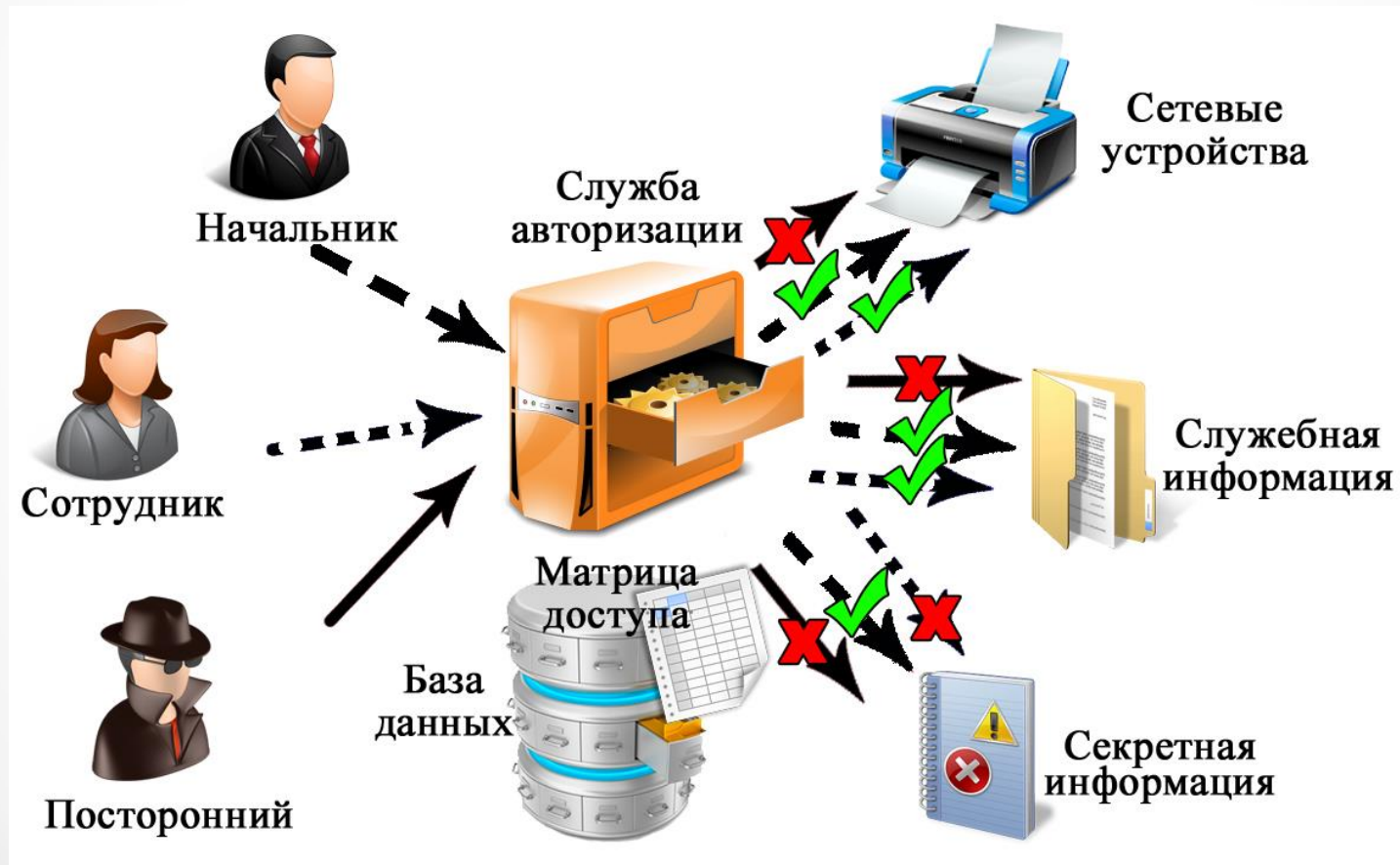
Принципы организации разграничения доступа

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

Принципы организации разграничения доступа

Схема реализации дискреционного управления доступом

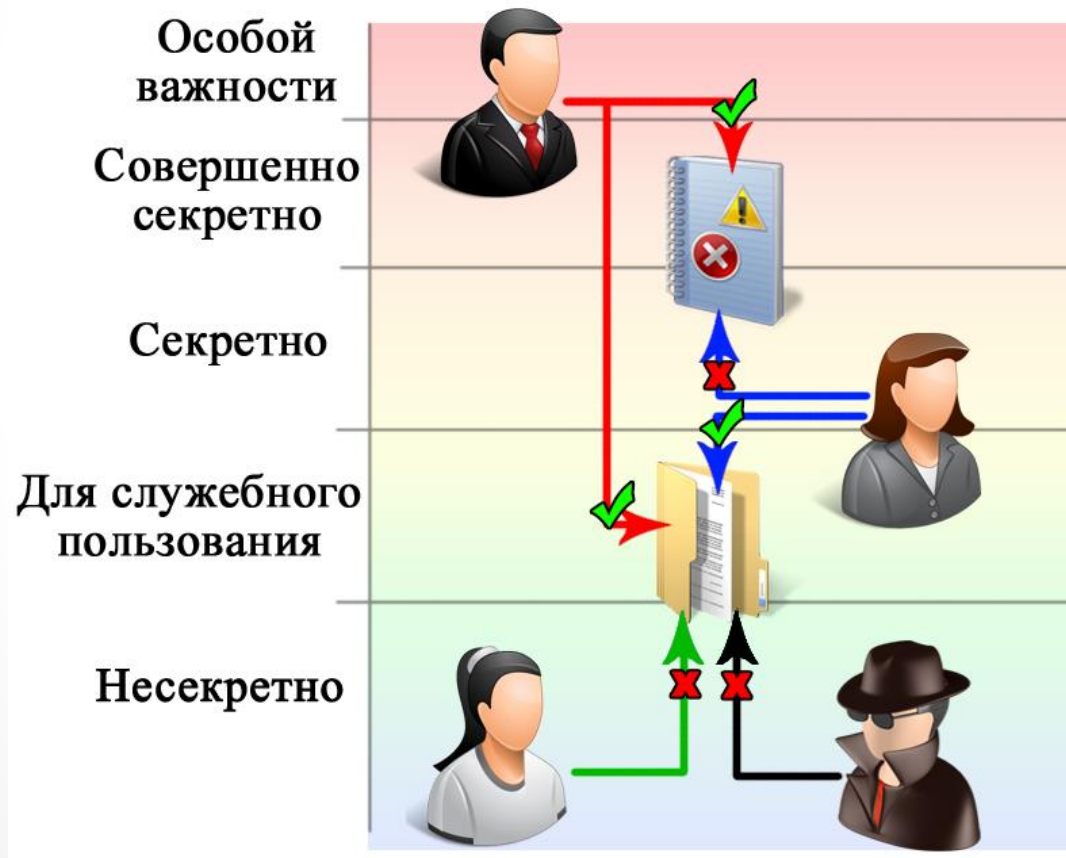


Принципы организации разграничения доступа

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.

Принципы организации разграничения доступа

Схема реализации мандатного управления доступом



Принципы организации разграничения доступа

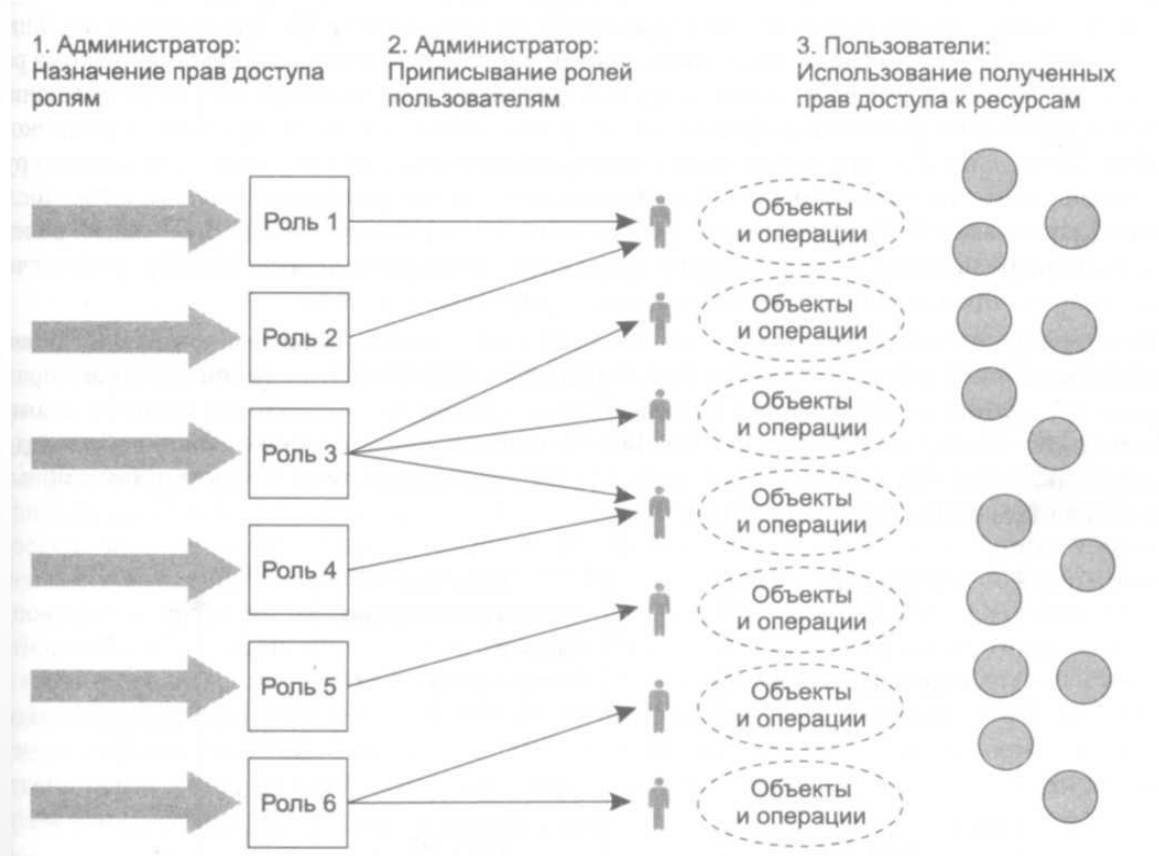
Ролевое управление доступом использует роли, которые по сути соответствуют понятиям «должность» и «круг должностных обязанностей».

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

Одна и та же роль может быть приписана разным субъектам.

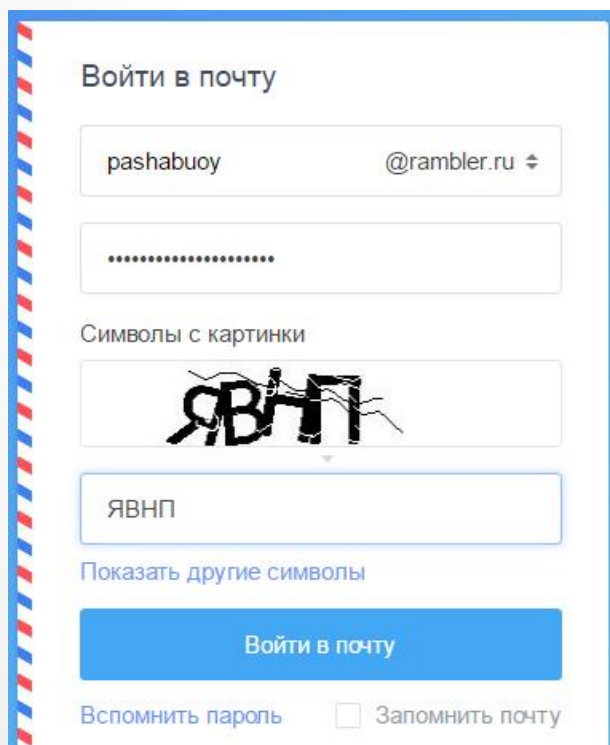
Принципы организации разграничения доступа

Схема авторизации в системах управления доступом на основе ролей



Применение методов разграничения доступа

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




Войти в почту

pashabuoy @rambler.ru ↕

.....

Символы с картинки

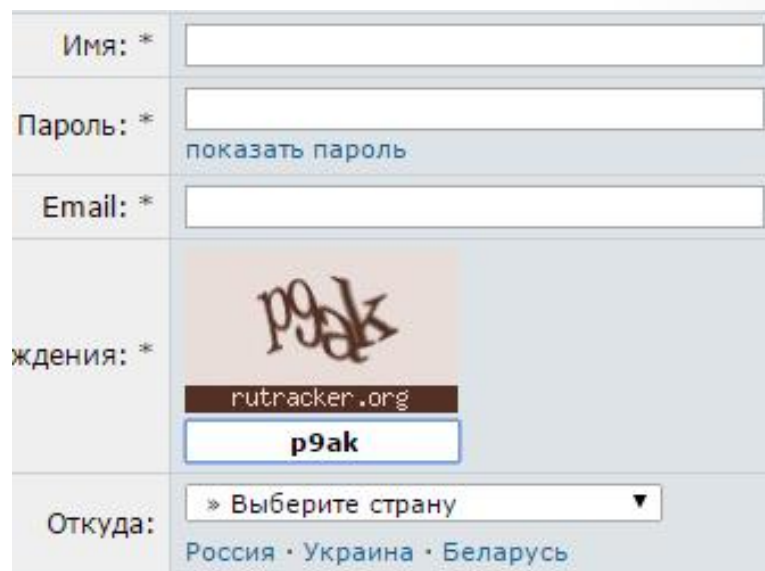


ЯВНП

Показать другие символы

Войти в почту

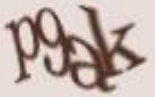
Вспомнить пароль Запомнить почту



Имя: *

Пароль: *
показать пароль

Email: *

ождения: * 
rutracker.org

Откуда:
Россия · Украина · Беларусь

Применение методов разграничения доступа

Пример дискреционного управления доступом на железнодорожной станции Ипуть БелЖД

Действия субъектов согласно ПРА	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».