



# Управление доступом на основе ролей

ГРУППА ПО-17(М)

ЗИМЦЕВ ПЁТР

# Общие сведения

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.

# РОЛИ

- ОПРЕДЕЛЯЕТ ЧЕТКИЕ ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА.
- ПОЗВОЛЯЕТ ФОРМИРОВАТЬ ГИБКОСТЬ РАСПРЕДЕЛЕНИЯ ДОСТУПОВ.
- ЯВЛЯЕТСЯ СОСТАВЛЯЮЩЕЙ СОВРЕМЕННЫХ СИСТЕМ.
- ИСПОЛЬЗУЕТСЯ В СИСТЕМАХ С ЧЕТКО ОПРЕДЕЛЕННЫМ КРУГОМ ДОСТУПОВ.
- ПРИВИЛЕГИИ ДОСТУПНЫ ПО СООТВЕТСТВУЮЩЕЙ РОЛИ.
- УПРОЩАЕТ РАБОТУ С ПЕРЕОПРЕДЕЛЕНИЕМ ДОСТУПОВ.

# История

- 1992 ГОД — СТАТЬЯ ФЕРРАЙОЛО И КУНА, ОПРЕДЕЛЯЮЩАЯ RBAC ПОСРЕДСТВОМ ДОСТУПА ТОЛЬКО ЧЕРЕЗ РОЛИ, ИЕРАРХИИ И ОГРАНИЧЕНИЯ. ФОРМАЛЬНАЯ МОДЕЛЬ [6];
- 1994 ГОД — DTOS БАЗИРОВАЛ ОПЫТНЫЙ ОБРАЗЕЦ RBAC, НА ПРОТОТИПЕ МОДЕЛИ, ПРЕДЛОЖЕННОЙ ФЕРРАЙОЛО, КУН, ГАВРИЛЬЯ (АНГЛ. GAVRILA)
- 1994 ГОД — СТАТЬЯ NYANCHAМА И OSBORN ОПРЕДЕЛЯЕТ МОДЕЛЬ;
- 1994 ГОД — ИВМ ПОДАЁТ (В ЕВРОПЕ) ПЕРВУЮ ЗАЯВКУ НА ПАТЕНТ В ОБЛАСТИ RBAC, ЦИТИРУЮЩУЮ ФЕРРАЙОЛО И КУНА;

# История

- 1995 ГОД — ФЕРРАЙОЛО, КУГИНИ (АНГЛ. CUGINI), КУН РАСШИРИЛИ ФОРМАЛЬНУЮ МОДЕЛЬ, ВВЕДЯ ОПРЕДЕЛЕНИЕ ФОРМ РАЗДЕЛЕНИЯ ОБЯЗАННОСТЕЙ [5];
- 1996 ГОД — МЕТОД САНДИ ДЛЯ ТОГО, ЧТОБЫ ОСУЩЕСТВИТЬ MAC НА ОСНОВЕ RВАС;
- 1997—1998 ГОДЫ — SYBASE, БЕЗОПАСНОЕ ВЫЧИСЛЕНИЕ, SIEMENS ОБЪЯВЛЯЕТ О ПРОДУКТАХ RВАС, ОПИСАННЫХ КАК БАЗИРУЮЩИЕСЯ НЕПОСРЕДСТВЕННО НА МОДЕЛИ

# История

- 1997 ГОД — БЕЗОПАСНОЕ ВЫЧИСЛЕНИЕ ВКЛЮЧАЕТ МОДЕЛЬ ФЕРРАЙОЛО-КУНА RVAC В АМЕРИКАНСКУЮ ГЛОБАЛЬНУЮ КОМАНДУ DOD И СИСТЕМУ УПРАВЛЕНИЯ; ВЫХОДИТ СТАТЬЯ КУНА НА ТЕМУ РАЗДЕЛЕНИЯ ОБЯЗАННОСТЕЙ, НЕОБХОДИМЫХ И ДОСТАТОЧНЫХ УСЛОВИЙ ДЛЯ БЕЗОПАСНОСТИ РАЗДЕЛЕНИЯ;
- 1997 ГОД — СТАТЬЯ ОСБОРНА ОСНОВАННАЯ НА ОТНОШЕНИЯХ МЕЖДУ RVAC И МНОГОУРОВНЕВОЙ БЕЗОПАСНОСТЬЮ МАНДАТНОЙ МОДЕЛИ ПОЛИТИКИ БЕЗОПАСНОСТИ; АННОТАЦИЯ РОЛИ, СВЯЗЫВАЮЩАЯ RVAC И МНОГОУРОВНЕВУЮ БЕЗОПАСНОСТЬ [4]
- 1998 ГОД — RVAC — МЕТОД КУНА ДЛЯ ТОГО, ЧТОБЫ ОСУЩЕСТВИТЬ RVAC НА СИСТЕМЕ MAC;
- 1999 ГОД — БАРКЛЕЙ (АНГЛ. BARKLEY), ФЕРРАЙОЛО, КУН ОТКРЫВАЮТ ИСХОДНЫЙ ОПЫТНЫЙ ОБРАЗЕЦ RVAC ДЛЯ РАЗВИТЫХ ВЕБ-СЕРВЕРОВ;

# Модель RBAC в 21 веке.

- 2000 ГОД — САНДИ, ФЕРРАЙОЛО, КУН ПУБЛИКУЮТ СТАТЬЮ, ОПРЕДЕЛЯЮЩУЮ ОБЪЕДИНЕННУЮ МОДЕЛИ RBAC, И ПРЕДЛАГАЮТ СТАНДАРТ RBAC;
- 2004 ГОД — АМЕРИКАНСКИЙ НАЦИОНАЛЬНЫЙ ИНСТИТУТ СТАНДАРТОВ И МЕЖДУНАРОДНЫЙ КОМИТЕТ ПО СТАНДАРТАМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ (ANSI/INCITS) ПРИНИМАЮТ ПРЕДЛОЖЕННУЮ САНДИ, ФЕРРАЙОЛО И КУНОМ МОДЕЛЬ RBAC КАК ЕДИНЫЙ СТАНДАРТ.

# Определение модели RBAC

- $S$  = СУБЪЕКТ
- $R$  = РОЛЬ
- $P$  = РАЗРЕШЕНИЯ
- $SE$  = СЕССИЯ
- $SA$  = НАЗНАЧЕНИЕ СУБЪЕКТА
- $PA: R \rightarrow 2P$  — ФУНКЦИЯ, ОПРЕДЕЛЯЮЩАЯ ДЛЯ КАЖДОЙ РОЛИ МНОЖЕСТВО ПРАВ ДОСТУПА; ПРИ ЭТОМ ДЛЯ КАЖДОГО  $P \in P$  СУЩЕСТВУЕТ  $R \in R$  ТАКАЯ, ЧТО  $P \in PA(R)$ ;
- $RH$  = ЧАСТИЧНО УПОРЯДОЧЕННАЯ ИЕРАРХИЯ РОЛЕЙ



# ЗАВИСИМОСТИ КОМПОНЕНТОВ РВАС

- ОДИН СУБЪЕКТ МОЖЕТ ИМЕТЬ НЕСКОЛЬКО РОЛЕЙ.
- ОДНУ РОЛЬ МОГУТ ИМЕТЬ НЕСКОЛЬКО СУБЪЕКТОВ.
- ОДНА РОЛЬ МОЖЕТ ИМЕТЬ НЕСКОЛЬКО РАЗРЕШЕНИЙ.
- ОДНО РАЗРЕШЕНИЕ МОЖЕТ ПРИНАДЛЕЖАТЬ НЕСКОЛЬКИМ РОЛЯМ.

# Описывая через теорию множеств

- $PA \subseteq P \times R$  ПРИ ЭТОМ РАЗРЕШЕНИЯ НАЗНАЧАЮТСЯ СВЯЗЯМ РОЛЕЙ В ОТНОШЕНИИ «МНОГИЕ КО МНОГИМ».
- $SA \subseteq S \times R$  ПРИ ЭТОМ СУБЪЕКТЫ НАЗНАЧАЮТСЯ СВЯЗЯМ РОЛЕЙ И СУБЪЕКТОВ В ОТНОШЕНИИ «МНОГИЕ КО МНОГИМ».
- $RH \subseteq R \times R$ , ОБОЗНАЧЕНИЕ:  $X \geq Y$  ОЗНАЧАЕТ, ЧТО  $X$  НАСЛЕДУЕТ РАЗРЕШЕНИЯ  $Y$ .

# Корреляция развития РВАС и закона Мура

ДЛЯ ВЫЯВЛЕНИЯ КОРРЕЛЯЦИИ БЫЛИ ИСПОЛЬЗОВАНЫ ДАТЫ РАЗВИТИЯ МОДЕЛИ РАСПРЕДЕЛЕНИЯ ДОСТУПА РВАС И ДАТЫ ЗАКОНА МУРА И ЕГО РАСШИРЕННЫХ ВЕРСИЙ.

В ИНСТРУМЕНТОМ РАСЧЕТА БЫЛ ИСПОЛЬЗОВАН MICROSOFT OFFICE EXCEL. КОЭФФИЦИЕНТ КОРРЕЛЯЦИИ РАВЕН 0.97177

# Список литературы

1. УПРАВЛЕНИЕ ДОСТУПОМ НА ОСНОВЕ РОЛЕЙ, [ЭЛЕКТРОННЫЙ РЕСУРС]. – РЕЖИМ ДОСТУПА: [HTTPS://RU.WIKIPEDIA.ORG/WIKI/УПРАВЛЕНИЕ\\_ДОСТУПОМ\\_НА\\_ОСНОВЕ\\_РОЛЕЙ](https://ru.wikipedia.org/wiki/УПРАВЛЕНИЕ_ДОСТУПОМ_НА_ОСНОВЕ_РОЛЕЙ).
2. RBAC АВТОРИЗАЦИЯ В YII И LDAP, [ЭЛЕКТРОННЫЙ РЕСУРС]. – РЕЖИМ ДОСТУПА: [HTTPS://HABR.COM/RU/POST/177873/](https://habr.com/ru/post/177873/)
3. ДОСТУП К САЙТУ НА ОСНОВЕ РОЛЕЙ (RBAC) В YII2, [ЭЛЕКТРОННЫЙ РЕСУРС]. – РЕЖИМ ДОСТУПА: [HTTPS://KLISL.COM/RBAC.HTML](https://klisl.com/rbac.html)

# Список литературы

4. ROLE BASED ACCESS CONTROL IN THE WORLD WIDE WEB, [ЭЛЕКТРОННЫЙ РЕСУРС]. – РЕЖИМ ДОСТУПА: [HTTPS://CSRC.NIST.GOV/CSRC/MEDIA/PROJECTS/ROLE-BASED-ACCESS-CONTROL/DOCUMENTS/WEB\\_SERVERS/RBAC-WEB.PDF](https://csrc.nist.gov/csrc/media/projects/role-based-access-control/documents/web_servers/rbac-web.pdf)
5. ROLE-BASED ACCESS CONTROLS , [ЭЛЕКТРОННЫЙ РЕСУРС]. – РЕЖИМ ДОСТУПА: [HTTPS://CSRC.NIST.GOV/CSRC/MEDIA/PUBLICATIONS/CONFERENCE-PAPER/1992/10/13/ROLE-BASED-ACCESS-CONTROLS/DOCUMENTS/FERRAIOLO-KUHN-92.PDF](https://csrc.nist.gov/csrc/media/publications/conference-paper/1992/10/13/role-based-access-controls/documents/ferraiolo-kuhn-92.pdf)
6. ROLE-BASED ACCESS CONTROL MODELS, [ЭЛЕКТРОННЫЙ РЕСУРС]. – РЕЖИМ ДОСТУПА: [HTTPS://CSRC.NIST.GOV/CSRC/MEDIA/PROJECTS/ROLE-BASED-ACCESS-CONTROL/DOCUMENTS/SANDHU96.PDF](https://csrc.nist.gov/csrc/media/projects/role-based-access-control/documents/sandhu96.pdf)