**Управление ролями пользователей**

1. **Титульный слайд (название модуля, автор)**

Приветствие. Занятие «Управление ролями пользователей».

1. **Программа модуля**

Кратко – про что будет доклад. На практическом занятии: знакомство с процессом извлечения ролей (role mining), рассмотрение типовых алгоритмов role mining, оптимизация результата.

1. **Реализация разграничения доступа в компьютерной системе**

Ввести понятие монитора безопасности, как основного метода разграничения доступа в КС.

Ссылки:

Н.А. Гайдамакин, «Учебно-методический комплекс. Теоретические основы компьютерной безопасности», раздел 1.3.

1. **Политика разграничения доступа**

Ввести множество всех возможных доступов (P), которое делится на 2 класса (легитимные и нелегитимные доступы). Ввести понятие политики разграничения доступа как способа задания класса легитимных доступов.

Рассказать о матрице доступа на примере дискреционного доступа.

Рассказать о мандатной модели на примере упрощенной модели Белла Лападулы (правила No read up и No write down).

Н.А. Гайдамакин, «Учебно-методический комплекс. Теоретические основы компьютерной безопасности», разделы 2.1, 2.2.

1. **Процесс управления доступом**

Ввести общее понятия процесса управления доступом и дать обзор его процедур.

Пояснить, что он относится к процедурному уровню обеспечения ИБ.

Ссылки: <https://www.invensislearning.com/blog/itil-access-management/>

1. **Процесс управления доступом**

Пояснить какие варианты запроса доступа могут быть (различные виды инициации процесса управления доступом).

1. **Процесс управления доступом**

Уточнить, что проверка разбивается на две подпроцедуры: кто инициировал запрос (точно ли тот, за кого он себя выдает) и собственно, легитимность самого запроса – можно ли предоставить доступ, фигурирующий в запросу.

1. **Процесс управления доступом**

Пояснить, что процедура корректировки доступа в КС одна из самых быстрых и не требующих больших трудозатрат, но при этом чаще всего пытаются автоматизировать именно эту процедуру.

1. **Процесс управления доступом**

Отметить, что предоставление доступа – это далеко не конец процесса.

Привести примеры основных событий, требующих пересмотра прав доступа: отпуск, смена должности, перевод в другое подразделение и пр.

1. **Процесс управления доступом**

Отметить, что доступы также рекомендуется журналировать, но акцентировать внимание на затратах, связанных с журналированием (нагрузка на оборудование, необходимость хранения журналов).

Также отметить, что, помимо выявления подозрительных действий, журналирование – хороший способ получения информации для актуализации прав доступа (например, удаления неиспользуемых прав у пользователя).

1. **Процесс управления доступом**

Отметить, что задача прекращения доступа может быть даже сложнее, чем задача предоставления доступа. Так как при блокировании доступа надо учесть все виды предоставленного доступа, а также различные изменения, которые вносились по ходу мониторинга (например, передача прав заместителю и пр.).

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **Проблемы практической реализации управления доступом**

Процесс предоставления доступа порождает противоречие при попытках его оптимизации:

С одной стороны, сложность процесса предполагает необходимость укрупнения прав – например, давать доступ к целой компьютерной системе разом.

С другой стороны, есть базовые принципы наименьших привилегий и подход «запрещено все, что не разрешено явно» - это требует делать гранулированные права доступа.

Но без укрупнения прав не обойтись – если согласовывать индивидуальные доступы к сотням тысяч объектов защиты, это займет годы, что противоречит здравому смыслу.

Таким образом, надо решать задачу укрупнения прав, но с соблюдением принципа минимальных привилегий и пр.

1. **Кто согласует доступ?**

Пояснить, что для организации, в первую очередь, существуют бизнес-процессы. Процессы делятся на отдельные операции. И что у процессов, что у операций есть хозяева – лица, ответственные за все, в том числе, за предоставление полномочий персоналу.

1. **Кто согласует доступ?**

Внутри бизнес-операции силами хозяина можно определить задействованные информационные активы и компьютерные системы, а также субъектов доступа – персонал операции. Именно хозяин(владелец) должен определять правила корректного использования активов и выстраивать работу персонала в рамках операции.

Таким образом, именно хозяева операций – основные согласующие доступ лица для активов, которые задействованы в их операции. Также хозяева операций могут назвать отличия доступа разных ролей персонала внутри своей операции.

Ссылки:

ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», раздел 7.

1. **Что нужно чтобы найти владельцев активов?**

Отметить, что в реальной жизни процесс поиска владельца активов непрост: он предполагает, что в организации высокий уровень зрелости процессов, а это далеко не всегда так. Нередко в организации не выполнен даже первый шаг: идентификация процессов и назначение хозяев.

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **Ролевая модель управления доступом**

Идея ролевой модели управления доступом – объединить в рамках одной сущности сразу много объектов и операций (видов доступа). При этом пару «операция», «объект» будем называть транзакцией. При описании ролевой модели, как правило, используют именно транзакции, а не отдельно объекты и отдельно операции.

1. **Как формируется роль?**

Отметить, что роль достаточно естественно формируется из описания процесса (операции). При этом не нарушается принцип минимальности привилегий, так как в роль включаются именно те транзакции, что нужны для выполнения операции. Уменьшение множества транзакций хотя бы на один элемент приведет к невозможности выполнения операции.

Опять отметить, что все это верно только при наличии хорошо задокументированных процессов в организации.

1. **Стандарт Role-based access control (RBAC)**

Познакомить со стандартом RBAC – наиболее знаменитым стандартом, описывающим принципы ролевого управления доступом.

Упомянуть про уровни RBAC и образуемую ими «решетку».

Ссылки: <https://csrc.nist.gov/Projects/Role-Based-Access-Control>

1. **RBAC. Иерархия ролей**

Отметить, что нередко роли могут вкладываться друг в друга – при этом нижележащая роль включает в себя все транзакции роли-предка.

1. **RBAC. Ограничения**

Также отметить, что RBAC отличает роли авторизованные (которые потенциально назначены пользователю) и активные (те, которые пользователь использует в настоящий момент времени). Такой подход позволяет проводить дополнительные проверки правил разделения полномочий и блокировать активацию роли, если возникает такое нарушение.

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **Процесс управления доступом**

Заметить, что при переходе к ролевой модели сам процесс управления доступом особо не меняется. Отличие только в том, что теперь запрашивается и предоставляется не отдельный доступ к объекту, а сразу роль.

1. **Связь с процессом управления ролями**

Также отметить, что для ролевой модели управления доступом нужен каталог ролей, который нужно поддерживать в актуальном состоянии. Это приводит к необходимости реализации отдельного процесса – управления ролями.

1. **Процесс управления ролями**

Процесс начинается с первичного заполнения каталога ролей. Это наиболее трудоемкий шаг, на всех последующих итерациях он будет требовать на порядки меньших трудозатрат.

При этом есть два способа наполнения: сверху вниз – от бизнес процессов и снизу вверх – от фактически назначенных транзакций.

1. **Процесс управления ролями**

В организации не бывает абсолютно одинаковых работников. А значит и обязанности хоть немного, но будут отличаться. Это приводит к тому, что роль может иметь вполне типовое наполнение транзакциями, но у отдельных сотрудников будут возникать свои отклонения от основной роли – исключения. Все исключения должны идентифицироваться и уточняться. Возможно, исключение может быть отброшено и наблюдаемое отклонение просто следствие некорректного предоставления доступа работнику.

1. **Процесс управления ролями**

Предыдущие шаги являются зоной ответственности выделенного аналитика ролевой модели организации, а хозяева процессов и операций выступают лишь в роли консультанта. Но шаг «сертификация ролей» выводит хозяев на первый план – именно они должны рассмотреть результаты работы аналитиков ролевой модели и принять или не принять сформированные роли.

1. **Процесс управления ролями**

После завершения формирования каталога ролей в него неизбежно будут вносится изменения: меняются процессы, инструменты, организационно-штатная структура. Внесение изменений в ролевую модель запускает весь цикл процесса по новой.

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **Построение ролевой модели сверху вниз**

Построение ролевой модели сверху вниз – очень трудоемкий процесс, но он гарантирует наилучший результат. Пояснить, что здесь мы идем от более крупных сущностей к меньшим: анализируя процесс, определяем состав операций в нем, далее определяем бизнес-роли – т.е. различные наборы обязанностей персонала, задействованного в операции. На основе бизнес ролей и сведений об автоматизации операции выясняем набор системных ролей (т.е. непосредственно сущностей отдельных КС), из которых состоит бизнес роль. После этого можно сформировать конкретные наборы транзакций, входящие в системную роль.

Самое важное, что при таком подходе проще всего преодолеть границу «бизнеса» и «техники», т.е. тот масштаб формирования ролевой модели, где зона ответственности от представителей бизнес-подразделений переходит к представителям ИТ-подразделения.

1. **Построение ролевой модели сверху вниз – алгоритм**

Пройти по шагам алгоритма. Еще раз отметить, что он трудоемок, так как выполняется вручную и требует участия руководителей различного уровня.

1. **Построение ролевой модели снизу вверх**

Описать вариант снизу вверх, когда мы движемся от транзакций в сторону процесса. Этот подход хорош тем, что первые шаги достаточно легко автоматизируются (сбор текущих назначений прав, формирование системных ролей на их основе).

Но отметить, что в этом подходе очень сложно преодолеть «границу бизнеса и техники». Особенно, если в организации низкий уровень зрелости управления процессами.

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **Общие подходы к извлечению ролей**

Остановиться на общих принципах role mining: мы не смотрим внутрь системы, для нас она – просто набор доступных транзакций.

Системные роли в большинстве случаев будут плоским списком, а вся иерархия будет реализовываться на уровне бизнес ролей.

И отметить, что границей role mining является именно построение системных ролей.

1. **Извлечение ролей: входные и выходные данные**

Проговорить входные данные и RBAC-состояние. Пояснить суть каждого элемента.

Ссылки:

SACMAT '09: Proceedings of the 14th ACM symposium on Access control models and technologies, June 2009 Pages 95–104, <https://doi.org/10.1145/1542207.1542224>

1. **Извлечение ролей: оценка качества результата**

Ввести взвешенную структурную сложность RBAC-состояния, напомнить понятия транзитивного замыкания и L1 нормы. Заметить, что для матриц RBAC-состояния L1 норма – это просто количество единиц.

Продемонстрировать разные оптимизационные задачи, задаваемые разными значениями вектора W

Ссылки:

SACMAT '09: Proceedings of the 14th ACM symposium on Access control models and technologies, June 2009 Pages 95–104, <https://doi.org/10.1145/1542207.1542224>

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **Последующие задачи**

Отметить, что есть также много других задач, связанных с управлением ролями, где могут применяться технологии искусственного интеллекта и машинного обучения.

В частности, сопоставление системных и бизнес ролей на основе различных атрибутов пользователя (должность, место работы, положения должностной инструкции и т.д.).

Отметить, что многие из этих задач значительно сложнее первичного извлечения ролей и в настоящее время там нет универсальных решений.

1. **Спасибо за внимание.**

Рекомендуемая литература:

1.