УДК 004 EDN QAIVQZ

https://www.doi.org/10.47813/mip.5.2023.9.5-9

Задача создания инфраструктуры классов политики управления пользователями

Б.С. Самандаров[1*], Ш.Х. Тажибаев[2]

[1]Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий, Ташкент, Узбекистан
[2]Каракалпакский государственный университет им. Бердаха, Нукус, Узбекистан

*E-mail: batirbeksamandarov@gmail.com

Аннотация. В статье описывается разработка и реализация системы управления пользователями, основанной на классах политики. Авторы представляют методологию построения такой системы, а также описывают ее основные компоненты и функции. В статье рассматриваются основные классы, которые могут входить в структуру политики управления пользователями, примеры использования классов политики для решения задач управления пользователями в различных сферах деятельности, таких как корпоративные сети, образовательные учреждения и государственные организации. Результаты исследования показывают, что использование классов политики может значительно упростить процесс управления пользователями и повысить эффективность работы системы.

Ключевые слова: политика управления пользователями, инфраструктура классов, управлением ролями пользователей.

The task of creating a user management policy class infrastructure

B.S. Samandarov[1*], Sh.X. Tajibaev[2]

[1]Tashkent University of Information Technologies named after Muhammad al-Khorazmiy, Tashkent, Uzbekistan
[2]Karakalpak State University named after Berdakh, Nukus, Uzbekistan

*E-mail: batirbeksamandarov@gmail.com

Abstract. The article describes the development and implementation of a user management system based on policy classes. The authors present the methodology for building such a system, as well as describe its main components and functions. The article discusses the main classes that can be included in the structure of user management policy, examples of using policy classes to solve user management problems in various fields of activity, such as corporate networks, educational institutions and government organizations. The results of the study show that the use of policy classes can significantly simplify the user management process and increase the efficiency of the system.

Keywords: user management policy, class infrastructure, user role management.

1. Введение

В современном мире информация играет ключевую роль во многих сферах деятельности, включая бизнес, науку, образование, медицину, правительственные организации и многое другое. Несоблюдение правил доступа и недостаточная защита информационных систем могут привести к серьезным последствиям, таким как утечка конфиденциальных данных, нарушение работы системы и потеря доверия клиентов и партнеров.

Исследование показывает, что средние затраты на утечку данных составляют $3.92 млн. Однако, если организация имеет хорошо разработанные политики управления пользователями, затраты могут быть снижены на $1.23 млн. Также было выявлено, что организации с хорошо разработанными политиками управления пользователями имеют меньше вероятности стать жертвой кибератак [1].

Согласно исследованию IBM, средняя стоимость утечки данных достигла рекордно высокого уровня в 2023 году и составила 4,45 миллиона долларов США. Это на 2,3% больше по сравнению с затратами на 2022 год в размере 4,35 млн долларов США. Долгосрочная средняя стоимость выросла на 15,3% по сравнению с 3,86 млн долларов, указанными в отчете за 2020 год [2].

Поэтому проектирование инфраструктуры класса политик управления пользователями является приоритетной задачей для любой организации, которая работает с информационными системами. Эта инфраструктура включает в себя набор правил и процедур, которые регулируют доступ к информации и управляют поведением пользователей в информационной системе.

2. Основная часть

Один из основных компонентов инфраструктуры класса политик управления пользователями – это система авторизации и аутентификации, которая обеспечивает контроль доступа к информации на основе уровня доступа пользователя. Это может быть реализовано через пароли, токены или биометрическую аутентификацию.

Обеспечение жесткого контроля доступа пользователей с помощью управления идентификацией является важным шагом в процессе разработки надежного плана обеспечения безопасности [3]. Проще говоря, управление идентификацией — это процесс обеспечения того, чтобы нужные люди имели доступ к нужным ресурсам в организации.

Исходя из вышеизложенного, возникает необходимость в проектировании инфраструктуры для управления ролями пользователей в информационной системе. Управление ролями пользователей является ключевым элементом в обеспечении безопасности информационных систем.

Управление ролями пользователей – это процесс определения ролей, назначения прав доступа и обеспечения безопасности системы, который позволяет эффективно управлять доступом к ресурсам в информационной системе. Этот процесс позволяет организациям контролировать, кто имеет доступ к каким ресурсам и какие действия с ними могут быть выполнены. Для этого необходимо определить роли пользователей, которые будут иметь доступ к системе, а также определить права доступа для каждой из этих ролей.

Одной из главных проблем, связанных с управлением ролями пользователей, является определение ролей и их соответствующих прав доступа. Необходимо определить, какие роли существуют в организации и какие права доступа имеет каждая из них. Это может быть достигнуто путем анализа бизнес-процессов и определения ролей, которые необходимы для выполнения этих процессов.

Инфраструктура классов политики управления пользователями должна быть гибкой и масштабируемой, чтобы можно было быстро и легко изменять права доступа в зависимости от изменяющихся требований и потребностей.

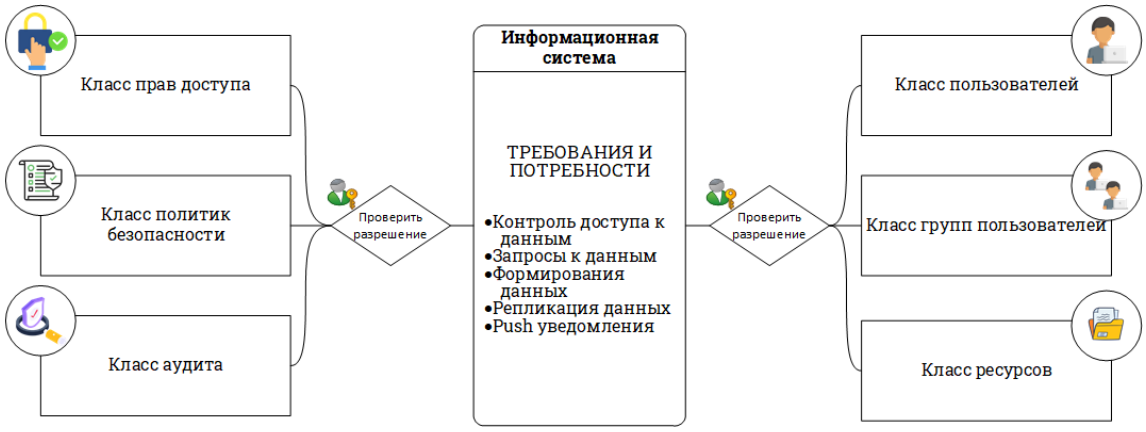

Рисунок 1. Инфраструктура классов политики управления пользователями.

Основные классы, которые могут входить в структуру политики управления пользователями, включают:

1. Класс пользователей – определяет всех пользователей системы и их свойства, такие как имя, пароль, права доступа и т.д.

2. Класс групп пользователей – группирует пользователей по определенным критериям, например, по отделу или роли в организации.
3. Класс ресурсов – определяет все ресурсы системы, к которым могут иметь доступ пользователи, такие как файлы, папки, базы данных и т.д.
4. Класс прав доступа – определяет права доступа пользователей к каждому ресурсу системы.
5. Класс политик безопасности – определяет правила и ограничения для доступа пользователей к ресурсам системы, такие как парольные политики, правила блокировки учетных записей и т.д.
6. Класс аудита – отслеживает действия пользователей в системе и сохраняет информацию о них для последующего анализа и мониторинга.

В зависимости от конкретных требований и потребностей системы, можно создавать дополнительные классы и наследовать их от основных классов. Например, для управления доступом к конфиденциальным данным можно создать класс "Конфиденциальные ресурсы" и определить права доступа только для определенных групп пользователей или индивидуальных пользователей. Также можно создать класс "Ограничения времени доступа", который определит правила доступа к ресурсам системы только в определенное время суток или в определенные дни недели.

Важно понимать, что структура классов политики управления пользователями должна быть гибкой и настраиваемой, чтобы обеспечивать максимальную безопасность и эффективность работы системы. При этом необходимо учитывать потребности и требования конкретной организации и ее пользователей.

5. Выводы

Таким образом, создание инфраструктуры классов политики управления пользователями является важным шагом в обеспечении безопасности и эффективности работы системы. Разработка и реализация такой инфраструктуры требует анализа потребностей бизнеса и технических возможностей системы, а также учета законодательных и регуляторных требований. В результате создания инфраструктуры классов политики управления пользователями повышается уровень безопасности, уменьшается вероятность ошибок и сбоев, а также облегчается администрирование системы.

Список литературы

1. Security Intelligence. What’s New in the 2019 Cost of a Data Breach Report. / [Электронный ресурс] https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/ (дата обращения: 18.07.2023).
2. IBM. Cost of a Data Breach Report 2023 / [Электронный ресурс] https://www.ibm.com/reports/data-breach (дата обращения: 10.08.2023).
3. Ishaq Azhar Mohammed. Systematic review of identity access management in information security / Ishaq Azhar Mohammed // International Journal of Innovations in Engineering Research and Technology. – 2017. – 4(7).