**НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ** **УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ** **«МОСКОВСКИЙ ФИНАНСОВО-ПРОМЫШЛЕННЫЙ УНИВЕРСИТЕТ** **“СИНЕРГИЯ”»**



|  |  |  |
| --- | --- | --- |
| **Факультет/Институт** |  | Информационных технологий |
|  |  | (наименование факультета/ Института) |
| **Направление/специальность** |  | Разработка, сопровождение и обеспечение безопасности информационных систем |
| **подготовки:** |  | (код и наименование направления /специальности подготовки) |
| **Форма обучения:** |  | очная |
|  |  | (очная, очно-заочная, заочная) |
|  |  |  |

**ЭССЕ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **на тему** |  | **Учетная запись пользователя** | | |
|  |  | (наименование темы) | | |
|  |  |  | | |
| **по дисциплине** | | |  | **Администрирование информационных систем** |
|  | | |  | (наименование дисциплины) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Обучающийся** |  | Буриев Р.Б. |  |  |
|  |  | (ФИО) |  | (подпись) |
| **Группа** |  | ВБИо-306-рсоб |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Преподаватель** |  | **Сибирев Иван Валерьевич** |  |  |
|  |  | (ФИО) |  | (подпись) |

**Москва 2024 г.**

В современном мире информационные системы стали неотъемлемой частью любой организации, играя ключевую роль в обработке, хранении и передаче данных. Основополагающим элементом администрирования информационных систем является учетная запись пользователя – персонализированный профиль, предоставляющий индивиду доступ к ресурсам системы. Учетная запись выступает своего рода цифровым удостоверением личности, определяющим, кто может получить доступ к системе и какие действия он вправе совершать. Ее важность трудно переоценить, поскольку от правильной организации и управления учетными записями напрямую зависит безопасность и эффективность работы всей информационной системы.

Учетные записи пользователей играют критическую роль в обеспечении безопасности, выступая первым рубежом защиты от несанкционированного доступа. Благодаря им администраторы могут контролировать, кто имеет доступ к конфиденциальной информации и какие операции разрешены каждому пользователю. Гибкая система управления учетными записями позволяет разграничивать права доступа, предотвращая утечки данных и защищая систему от вредоносных действий. Таким образом, учетные записи служат инструментом для поддержания целостности и конфиденциальности информации.

Существует несколько основных типов учетных записей, каждый из которых предназначен для выполнения определенных задач. Административные учетные записи предоставляют полный контроль над системой, учетные записи сотрудников обеспечивают доступ к необходимым для работы ресурсам, а гостевые учетные записи ограничивают доступ к минимальному набору функций. Правильное распределение пользователей по типам учетных записей позволяет оптимизировать работу системы и минимизировать риски безопасности.  
  
Управление учётными записями пользователей — критически важный аспект безопасности любой системы. Оно включает в себя несколько ключевых компонентов: идентификацию, аутентификацию, авторизацию и управление жизненным циклом. Идентификация пользователя отвечает на вопрос «кто это?» и реализуется через уникальные идентификаторы, такие как логин, ID или другие специфические для системы атрибуты. Аутентификация подтверждает заявленную личность, чаще всего с помощью паролей, хотя все большее распространение получают более надежные методы, такие как многофакторная аутентификация и биометрия. После успешной аутентификации вступает в действие авторизация, определяющая, что именно пользователь может делать в системе. Это достигается через разграничение прав доступа, назначение пользователей в группы и определение ролей. Наконец, управление жизненным циклом учётной записи включает в себя процессы создания, изменения, блокировки и удаления учётных записей, обеспечивая актуальность и безопасность системы на протяжении всего времени существования пользователя в ней.

Системы используют различные типы учётных записей, каждый из которых предназначен для определённых целей. Локальные учётные записи существуют только на конкретном устройстве и предоставляют доступ к ресурсам этого устройства. Доменные учётные записи, напротив, управляются централизованно в рамках домена и позволяют пользователю получать доступ к ресурсам сети, к которой принадлежит домен. Учётные записи служб используются приложениями или службами для выполнения своих функций, часто без взаимодействия с пользователем. Гостевые учётные записи предоставляют ограниченный временный доступ к системе. Административные учётные записи наделены широкими полномочиями для управления системой, в то время как привилегированные учётные записи имеют ещё более высокий уровень доступа и используются для выполнения критически важных задач. Выбор типа учётной записи зависит от конкретных потребностей и сценариев использования. Например, для домашнего компьютера подойдут локальные учётные записи, в корпоративной среде — доменные, а для выполнения фоновых задач — учётные записи служб.

Безопасность учётных записей — фундаментальный аспект защиты информации. Строгие политики паролей, включающие требования к сложности, сроку действия и истории использования, существенно снижают риск компрометации. Многофакторная аутентификация добавляет дополнительные уровни защиты, требуя от пользователя подтверждения личности несколькими способами. Аудит учётных записей позволяет отслеживать активность пользователей, выявлять аномалии и потенциальные угрозы. Комплексный подход к защите от несанкционированного доступа, включающий меры по предотвращению взлома и кражи учётных данных, необходим для обеспечения целостности и конфиденциальности информации. Эффективное управление учётными записями в организации предполагает централизованный подход, обеспечивающий единую точку контроля и администрирования. Делегирование полномочий позволяет распределять ответственность за управление учётными записями, оптимизируя рабочие процессы. Интеграция с другими системами, такими как HR-системы или системы управления доступом, упрощает управление и синхронизацию данных. Автоматизация процессов управления учётными записями, например, автоматическое создание и удаление учётных записей при приёме и увольнении сотрудников, повышает эффективность и снижает вероятность ошибок. В заключение, грамотное управление учётными записями пользователей является краеугольным камнем безопасности и эффективности любой организации. Оно обеспечивает защиту данных, контроль доступа к ресурсам и стабильность работы систем. Перспективы развития технологий управления учётными записями направлены на повышение уровня автоматизации, интеграции с искусственным интеллектом и усиление безопасности. Облачные технологии играют всё более важную роль, предоставляя гибкие и масштабируемые решения для управления учётными записями, открывая новые возможности для централизованного контроля и автоматизации процессов.