**НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«МОСКОВСКИЙ ФИНАНСОВО-ПРОМЫШЛЕННЫЙ УНИВЕРСИТЕТ «СИНЕРГИЯ»**

|  |  |  |
| --- | --- | --- |
| **Факультет/Институт** |  | Информационных технологий |
|  |  | (наименование факультета/ Института) |
| **Направление/специальность** |  | Информационные системы и технологии |
| **подготовки:** |  | (код и наименование направления /специальности подготовки) |
| **Форма обучения:** |  | очная |
|  |  | (очная, очно-заочная, заочная) |
|  |  |  |

**ЭССЕ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **по дисциплине** |  | Золотые правила администратора | | |
|  | | |  | (наименование дисциплины) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Обучающийся** |  | **Фиников Дмитрий Сергеевич** |  |  |
|  |  | (ФИО) |  | (подпись) |
| **Группа** |  | **группа ВБИо-308рсоб** |  |
|  |  |  |  |

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

**Москва 2024 г.**

**1. Избегайте экспериментов на работающей системе**

Никогда не проводи экспериментов на работающей системе. Если это все-таки необходимо, сначала сделай полный бэкап.

Не вносите изменения в работающую систему без подготовки, поскольку это может привести к критическим сбоям. Например, неправильное обновление программного обеспечения на сервере может лишить пользователей доступа. Если изменения все-таки необходимы, сначала создайте полный бэкап.

Лучше всего проводить такие работы, когда система используется минимально — например, ночью, в выходные или после окончания рабочего дня всех пользователей. Еще более безопасный подход — создать копию системы и развернуть ее в виртуальной среде для тестирования изменений, прежде чем вносить их в реальную систему.

**2. Всегда делайте полный бэкап перед изменением конфигурации сервера.**

Никогда не менять конфигурацию сервера, предварительно не сделав полный бэкап. Изменения в работающей системе без должной подготовки могут привести к критическим сбоям. Например, некорректное обновление программного обеспечения на сервере может вызвать потерю доступа для пользователей.

Перед установкой нового обновления операционной системы или любого другого критического изменения сначала создайте виртуальную копию всей системы для тестирования. Если тестирование проходит успешно, применяйте обновление на реальном сервере. В своей практике, например, при обновлении платформы 1С, я всегда использую Acronis для создания образов системы до и после обновления, чтобы иметь возможность быстро восстановить систему в случае возникновения непредвиденных проблем.

**3. Документируйте свои действия**

Всегда документируй свои действия в соответствующем журнале. Если это возможно, пользуйся встроенными в ОС средствами аудита. Ведение журналов помогает отслеживать изменения и быстро находить причины проблем. Это также полезно при передаче своих обязанностей другому администратору.

При установке нового сетевого устройства администратор фиксирует все этапы настройки, включая такие детали, как IP-адреса и порты. Эти данные заносятся в журнал, который хранится в облачном хранилище, обеспечивая доступность информации из любой точки. Ведение такой подробной документации помогает быстро восстановить настройки в случае сбоев и служит полезным справочником для будущих изменений.

Кроме текстовых записей, рекомендуется также делать скриншоты каждого этапа настройки. Визуальная документация облегчает понимание и повторение процессов, уменьшает зависимость от человеческой памяти и снижает вероятность ошибок в будущем. Это особенно полезно в сложных системах, где одна небольшая ошибка может привести к серьезным последствиям. Таким образом, продуманное ведение журналов и визуальная документация способствуют более надежному и безопасному управлению системами.

**4. Перераспределяйте задачи, но осторожно.**

Если можно переложить часть работы на подчиненного – сделай это. Но, если ты не уверен, что подчиненный справится с заданием должным образом – сделай это сам.

Делегирование задач позволяет эффективно управлять временем и ресурсами. Однако важно тщательно выбирать, кому поручать конкретные задачи, чтобы они были выполнены качественно и в срок. Различные задачи требуют разного уровня опыта и навыков; поэтому их следует поручать сотрудникам, которые могут с ними справиться.

Например, администратор может поручить младшим сотрудникам регулярное обновление антивирусного ПО, что позволяет освободить свое время для более сложных задач, таких как настройка и поддержание сетевой безопасности. Это распределение обязанностей позволяет гарантировать, что система будет надежно защищена, и при этом каждый участник команды будет развивать свои профессиональные навыки, работая в соответствии со своим уровнем компетенции. Делегирование также способствует развитию сотрудников, предоставляя им возможность учиться и приобретать новые навыки на практике.

**5. Соотнесение прав и ответственности.**

Всегда соотноси права с мерой ответственности, связанной с этими правами. Т.е. пользователь, имеющий больше прав, берет на себя больше ответственности. Администратор должен обладать полными правами на вверенную систему.

Права пользователя должны соответствовать его обязанностям и уровню ответственности, чтобы минимизировать риски злоупотреблений.

Например, инженеру поддержки может быть предоставлен доступ к инструментам мониторинга сети, чтобы он мог своевременно выявлять и сообщать о проблемах, однако права на изменение конфигурации оборудования остаются исключительно за старшим администратором. Такое распределение ролей предотвращает несанкционированные изменения и снижает вероятность ошибок.

Кроме того, для повышения безопасности рекомендуется, чтобы никто не работал под учетной записью администратора в повседневной деятельности. Это снижает риски случайных изменений и уменьшает потенциальные действия злоумышленников, которые могут получить доступ к системе. Задействование учетных записей с ограниченными правами для повседневных задач и использование административных учетных записей только в случае необходимости продуманных изменений помогает поддерживать стабильность и безопасность системы. Таким образом, четкое соотнесение прав и ответственности не только упрощает управление, но и способствует снижению рисков и повышению общей безопасности.

**6. Используйте учетную запись с ограниченными правами.**

При работе с ресурсами ИСВ в качестве пользователя используй учетную запись с обычными правами доступа.

Работа под учетной записью с минимальными правами — это важная практика, способствующая повышению безопасности и стабильности IT-систем. Она значительно снижает риски случайных изменений, а также защищает систему от потенциальных атак со стороны злоумышленников.

В повседневной работе, например при просмотре электронной почты или выполнении рутинных задач, администратору рекомендуется использовать обычную учетную запись с ограниченными правами. Это не только уменьшает вероятность случайных нарушений в системе, но и обеспечивает дополнительный уровень защиты в случае, если учетная запись будет скомпрометирована.

Переход на административную учетную запись должен происходить только при необходимости внесения значительных изменений или выполнения административных задач. Это позволяет контролировать доступ к критически важным функциям системы и минимизирует риск злоумышленников использовать привилегированные права для совершения атак.

Таким образом, стратегии разграничения прав способствуют улучшению безопасности и эффективному управлению системами. В результате администраторам удается поддерживать высокий уровень защиты данных и бесперебойную работу инфраструктуры, сводя к минимуму вероятность случайных ошибок и кибератак

**7. Регулярно меняйте пароли учетных записей.**

Регулярно меняй пароль учетной записи администратора, но не полагайся на свою память. Записывай пароль на бумаге и храни в месте с ограниченным доступом посторонних лиц.

Смена паролей на регулярной основе повышает безопасность системы, предотвращая несанкционированный доступ.

Например, администратор устанавливает ежемесячное напоминание о смене пароля и использует менеджер паролей для безопасного хранения новых паролей.

Эти расширенные золотые правила предоставляют администраторам ценные рекомендации по предотвращению распространенных ошибок, оптимизации работы и обеспечению безопасности и стабильности систем. Внедрение данных практик не только способствует улучшению управляемости информационных систем, но и значительно повышает их надежность.

Следование этим принципам помогает снижать риски, связанные с техническими сбоями и кибератаками. Это достигается за счет оптимального распределения прав доступа, регулярной смены паролей и использования учетных записей с минимальными привилегиями в повседневных задачах. Такой подход способствует созданию защищенной и стабильной рабочей среды.

Кроме того, использование проверенных процедур и политик управления IT-инфраструктурой укрепляет доверие пользователей и коллег. Они уверены в том, что система функционирует под надзором профессионалов, которые принимают меры для защиты данных и обеспечения бесперебойной работы. В результате, эти золотые правила не только помогают администраторам работать более эффективно, но и создают надежную и безопасную основу для всей организации.