13.3 Процесс: ACCESS MANAGEMENT - Управление доступом

Управление доступом (Access Management) - процесс, отвечающий за допуск пользователей к использованию услуг, данных или других активов. *Управление доступом* помогает обеспечить *конфиденциальность*, *целостность* и доступность активов за счет того, что только авторизованные пользователи имеют возможность получить *доступ* или модифицировать *активы*. Основным драйвером процесса является *процесс Управления* информационной безопасностью, так как именно он формирует политики и правила, которые реализуются процессом Управления доступом.

Управление доступом **предоставляет ценность бизнесу благодаря тому, что:**

- Каждый сотрудник имеет уровень доступа, необходимый для выполнения своих обязанностей;
- Контролируемый доступ к активам позволит организации поддерживать необходимый уровень конфиденциальности информации;
- Уменьшение вероятности ошибочных действий при работе с данными или использовании критичной услуги;
- Аудит использования услуг и отслеживание некорректной работы с ними;
- Быстрое лишение прав при возникновении необходимости;
- Может понадобиться для обеспечения соответствия требованиям регуляторов.

Рассмотрим последовательность деятельностей для предоставления доступа.

1. **Запрос доступа** (или его ограничение) может быть осуществлен через следующие механизмы:
   - Стандартный запрос от отдела кадров (HR). Например, при найме нового сотрудника, увольнении, переводе в другой отдел и т.п.;
   - Запрос на изменение (RFC);
   - Запрос на обслуживание переданный рассмотренным выше процессом управления запросами на обслуживание;
   - В процессе выполнения авторизованного сценария или опции (например, скачивание приложения с центрального сервера).
2. **Верификация запроса на получение доступа** включает в себя проверку двух категорий:
   - Пользователь, запрашивающий доступ, действительно тот, за кого себя выдает;
   - Пользователь, запрашивающий доступ, имеет право его получить;

Первый пункт проверяется обычно с помощью предоставления имени и пароля - они доказывают то, что пользователь является легитимным. В некоторых организациях могут быть использованы eToken, биометрическая аутентификация и т.п.

Идентификатор (Identity) *- уникальное наименование, используемое для идентификации пользователя, человека или роли. Идентификатор используется для предоставления прав пользователю, человеку или роли.*

Примерами идентификации могут быть имя пользователя Иванов Иван или Роль "Менеджер Изменений".

Вторая категория требует некоторой независимой проверки, не связанной с запросом. Например:

- Уведомление от Отдела кадров о том, что это новый сотрудник и ему необходим доступ к стандартному набору услуг;
- Уведомление от Отдела кадров о том, что сотрудник получил повышение по службе и ему необходим доступ к дополнительным услугам;
- Подтверждение от соответствующего процессу менеджера;
- Предоставление запроса на обслуживание (с обоснованием) через сервис-деск;
- Предоставление запроса на изменение через процесс Управления изменениями;
- Политика безопасности, в которой оговорено то, что пользователи могут получить доступ к услугам, если они им необходимы.

Для новых услуг должны быть четко определены пользователи и группы, которые будут иметь к ним доступ.

3. **Предоставление доступа.** Управление доступом не принимает решений относительно того, кто и куда будет иметь доступ. Процесс только реализует политики и правила, определенные на этапах Проектирования или Построения стратегии. После верификации пользователя, Управление доступом предоставит ему доступ для использования запрошенной услуги. В большинстве случаев непосредственное предоставление доступа требует действий со стороны каждой команды, поддерживающей услугу. Поэтому при проектировании услуг лучше предусмотреть автоматизацию процесса предоставления доступа.
4. **Мониторинг статуса идентичности**

Пользователи, работающие в организации, и их роли могут меняться. Примерами изменения могут быть:

- Изменение обязанностей - в этом случае пользователю может понадобиться доступ к другому набору услуг или просто к дополнительным услугам;
- Повышение или понижение в должности - в этом случае пользователю обычно необходим доступ к тому же набору услуг, но с другими уровнями;
- Перевод - в этом случае пользователю чаще всего нужен будет тот же набор услуг, но в другом регионе и с другими данными;
- Отставка или смерть - в этом случае все доступы должны быть немедленно аннулированы;
- Выход на пенсию - в этом случае доступы либо аннулируются, либо ограничиваются. Например, сотрудник, вышедший на пенсию, может иметь доступ к услугам по покупке продуктов своей компании по сниженной цене;
- Дисциплинарное ограничение - временное ограничение доступа пользователя из-за какой-то провинности;
- Увольнение - в этом случае доступы должны быть немедленно аннулированы во избежание инцидентов безопасности.

5. **Мониторинг доступа**

Управление доступом ответственно не только за непосредственное предоставление доступа, но и за контроль его использования. Поэтому функция контроля доступа должны быть

предусмотрена в рамках деятельностей мониторинга. Если возникают какие-то нарушения, они характеризуются как инциденты безопасности. Управление доступом принимает участие в определении настроек систем обнаружения вторжений (IDS).

6. Отзыв или ограничение прав

Наряду с предоставлением доступа, Управление доступом ответственно за его аннулирование или ограничение.

Аннулирование доступа происходит в таких случаях как смерть, увольнение, сокращение, кардинальное изменение обязанностей и т.п.

В ряде случаев полностью лишать сотрудника доступов не требуется, но есть необходимость в их ограничении. Например, при понижении сотрудника в должности.

13.4. Взаимосвязь процессов Эксплуатации с другими этапами жизненного цикла Управление изменениями

Несмотря на то, что Управление изменениями рассматривается в рамках этапа Преобразования, персонал Эксплуатации услуг должен принимать участие в следующем:

- Инициализация и передача на рассмотрение Запросов на изменения (RFC), которые позволят разрешить проблемы, возникающие в процессе Эксплуатации;
- Участие во встречах с руководством для обсуждения позиции, рисков и проблем Эксплуатации;
- Участие в реализации изменений в соответствии с предписаниями Управления изменениями;
- Осуществление "откатов" в соответствии с предписаниями Управления изменениями (в случае неудачных изменений);
- Обеспечивать поддержку в определении и управлении моделей изменений, которые имеют отношение к компонентам и услугам этапа Эксплуатации;
- Получение расписаний изменений и подготовка к ним персонала;
- Использование процесса Управления изменениями для стандартных операционных изменений.

- **Управление конфигурациями**

Также как и Управление изменениями, Управление конфигурациями рассматривается в рамках этапа Преобразования. Тем не менее, персонал Эксплуатации услуг вовлечен в следующее:

- Информирование Управление конфигурациями о найденных несовпадениях между фактическим состоянием конфигурационных единиц и информацией в Системе управления конфигурациями (CMS);
- Осуществление действий по исправлению найденных несоответствий под контролем Управления конфигурациями.

- **Управление релизами и развертыванием**

Персонал Эксплуатации участвует в следующем:

- Осуществление всех необходимых действия под контролем Управления релизами и развертыванием в вопросах, касающихся компонентов и услуг этапа Эксплуатации;
- Участие в планировании значительных релизов для того, чтобы были учтены все проблемы, которые могут возникнуть непосредственно на этапе Эксплуатации;
- Помещение/удаление компонентов в Библиотеку эталонного ПО (DML).

- **Управление мощностями**

Как мы уже знаем, Управление мощностями работает на трех уровнях - Управление мощностями бизнеса, Управление мощностями услуг, Управление мощностями ресурсов:

- В рамках Управления мощностями бизнеса персонал Эксплуатации взаимодействует с представителями бизнеса для планирования/обсуждения долгосрочных и краткосрочных вопросов и проблем, которые могут затронуть мощности IT;
- В рамках Управления мощностями услуг этап Эксплуатации помогает более детально оценить характеристики каждой услуги, а также потребность пользователей или транзакций в услугах и инфраструктуре (в частности, в зависимости от времени);
- В рамках Управления ресурсами этап Эксплуатации помогает более детально оценить показатели производительности/мощности, а также степень утилизации отдельных конфигурационных единиц.

Помимо рассмотренных аспектов, которые в большей степени имеют отношение к построению стратегии и планированию, операционный персонал выполняет ряд "повседневных" деятельностей, которые формально являются частью Управления мощностями, но осуществляются операционным персоналом.

- Мониторинг мощности и производительности для обнаружения проблем и предотвращения сбоев. Мониторинг должен быть максимально автоматизирован.
- Управление проблемами, связанными с производительностью и мощностью.
- Хранение данных Управления мощностями, которые формируются в процессе мониторинга.
- Управление спросом к отдельным ресурсам и услугам. Большинство вопросов управления спросом должно быть рассмотрено в рамках Проектирования, тем не менее, есть ряд вопросов, которые могут решаться на этапе Эксплуатации. Например, если с производительностью какой-то услуги возникают проблемы, персонал Эксплуатации услуг может ввести ограничение на количество пользователей, которые могут использовать услугу одновременно, до тех пор, пока проблемы не будут решены.
- Управление рабочей нагрузкой рассматривает вопросы оптимизации ресурсов инфраструктуры для увеличения производительности. Например, составление расписаний для отдельной услуги или ее перемещение с одних конфигурационных единиц на другие.
- Планирование мощностей. Персонал Эксплуатации услуг должен принимать участие в составлении планов мощностей.

- **Управление доступностью.**

На этапах Преобразования и Проектирования определяются уровни доступности, которые необходимо обеспечить для услуг. Этап Эксплуатации ответственен за непосредственное предоставление услуг на этих уровнях пользователям. При эксплуатации услуг может выясниться, что согласованные уровни доступности недостижимы или не являются оптимальными. Информация о несоответствиях поступает на этап Непрерывного улучшения услуг для осуществления корректирующих действий.
Кроме того, персоналу операционного уровня иногда необходимо проводить работы, которые требуют остановки услуг, например, для обновления. Расписание таких работ должно быть доведено до персонала Управления доступностью.

- **Управление знаниями.**

Информация с этапа Эксплуатации, которая имеет значение в перспективе, должна быть занесена в Систему управления знаниями по услугам (SKMS).

- **Финансовое управление.**

Персонал Эксплуатации услуг должен принимать участие в обосновании необходимости финансирования. Также при введении мер по сокращению издержек, в обязанности Эксплуатации услуг входит контроль за тем, чтобы эти меры не повлияли существенно на предоставление услуг.

- **Управление непрерывностью услуг.**

Эксплуатация услуг ответственна за тестирование планов восстановления и их реализацию в случае возникновения необходимости.