ОРГАНИЗАЦИЯ ВВОДА БОЛЬШИХ ОБЪЕМОВ ГЕОДАННЫХ

А.Ю. Константинов (ЦПИП «ВИСХАГИ-ЦЕНТР»)

В 1994 г. окончил факультет прикладной космонавтики МИИГАиК. В настоящее время — главный инженер ЦПИП «ВИСХАГИ-ЦЕНТР».

Одной из основных задач при организации цикла движения информации является задача сохранения данных на всех этапах выполнения проекта. Поэтому в этом случае огромное значение имеет принцип построения технологического цикла, правильное распределение прав доступа к информации и организация промежуточного, аварийного архивирования данных на ключевых этапах.

При организации производства на основе компьютерной сети Windows NT мы получаем инструментарий, позволяющий организовать практически любую комбинацию доступа к информации. В результате чего, мы выделяем руководителя проекта, наделяя его правами администратора, и исполнителей, с правами операторов. Используя возможность Windows NT организовывать сеть под управлением сервера, мы можем выделить дисковое пространство для хранения, группировки и архивного копирования особо ценной информации. Кроме того, каждому исполнителю выделяется объем дискового пространства для промежуточного хранения и регулярного архивирования информации в процессе выполнения работ. На выделенное пространство мы распределяем права доступа таким образом, чтобы ограничить возможность несанкционированного изменения и уничтожения информации для исполнителей, оставляя им возможность складирования результатов выполненных работ для дальнейшей проверки и обработки руководителем проекта.

На примере это может выглядеть следующим образом.

При выполнении работ по проекту «Медынь» организуется папка «Медынь», в которой, в свою очередь, создаются вложенные папки: «Проверка», «Планшеты», «Ортофотопланы», «Общая_информация», «Результат». В данном случае мы считаем, что работы по подготовке ортофотопланов (геокоординирование), планшетов, карт, планов и других материалов топоизученности (сканирование, трансформирование, геопривязка) выполнены. Необходимо создать карту на основе дешифрирования ортофотопланов или обновления старой картографической основы по ортофотопланам. Соответственно, существующие материалы распределяются по одноименным папкам, а необходимая дополнительная информация (инструкции, схемы объекта и наличествующих материалов и т. д.) располагается в папке «Общая_информация».

Распределяя права доступа для исполнителей, мы разрешаем только чтение папок «Планшеты», «Ортофотопланы», «Общая_информация», «Результат» и чтение и добавление в папку «Проверка». Тогда как для руководителя проекта мы устанавливаем полный доступ к общей папке «Медынь».

Кроме того, для каждого из исполнителей следует организовать его личные «операторские» папки, сгруппировав их под общей папкой «User», и дать исполнителям права на доступ только добавления и чтения.

В результате построенной выше схемы, исполнитель, находясь на рабочем месте, имеет возможность скопировать с сервера всю необходимую ему для работы исходную информацию, но не может ничего изменить или уничтожить. По окончанию выделенного ему объема работ оператор пересылает результат в папку «Проверка», для контроля и дальнейшей обработки ее руководителем проекта. Результат отсылается им в папку «Результат» для использования другими исполнителями, либо в целях складирования для архивного копирования.

В случае работы исполнителя над выданным ему объемом в течение нескольких дней, исполнитель выполняет ежедневное копирование в выделенную ему «операторскую» папку, с добавлением к названию файла даты производства работ. Следует отметить, что удаление отслуживших файлов не может быть выполнено самим исполнителем. Данную операцию может осуществлять только руководитель проекта, убедившись в полной непригодности информации.

Необходимой частью структуры хождения информации является ее архивное копирование. Запись удобнее всего осуществлять на ленту, автоматизировав этот процесс и настроив его на ночное время. В архивацию входят: папка проекта и личные «операторские» папки. Наиболее оптимальным вариантом является ежедневное архивирование на ленты (с комплектом лент на неделю) и ежемесячное копирование (с комплектом лент на год).

Описанная выше схема — базовая, но в связи с одновременным выполнением нескольких проектов, а также с большим количеством пользователей данной компьютерной сети необходимо перейти на более высокую ступень организации доступа к информации. Деления на руководителей проекта и операторов уже недостаточно, так как возрастает количество людей, наделенных правами для управления существующей информацией по выполняемым проектам. Поэтому необходим переход на систему разграничения доступа по конкретным сотрудникам, а не по группам администраторов и операторов.

В нашем примере для операторов ничего не меняется, но руководитель проекта ограничивается в своих полномочиях доступа к другим проектам. В результате, при увеличении количества пользователей системы мы ужесточаем доступ к информации, уменьшая тем самым риск ее потери или порчи.

Являясь основной при производственном цикле, информация по проектам не единственное, что требует разграничения прав. Так, например, неумелая или неграмотная настройка программного обеспечения может привести к сбоям или полной остановке рабочей станции, а в случае с сервером — и всей системы. Поэтому необходимо учитывать и ограничивать доступ и к системной информации, исключая случайную или преднамеренную перестройку и порчу программных продуктов, особенно на сервере.

Ряд мер по защите и организации передвижения производственной информации не должен ограничиваться разграничением прав доступа. Не стоит пренебрегать антивирусными программами и «инспекторами сети» — программами, отслеживающими в динамическом режиме кто и какими сетевыми ресурсами пользуется. Особое внимание следует уделить физическому доступу к серверу, а именно: ограничить ряд сотрудников, имеющих возможность даже подойти к нему. Желательно нахождение его в отдельной комнате и наличие повышенных мер защиты. Это связано с возможностью физического изъятия носителей информации с него, а также переустановки всей операционной системы, в результате чего права на информацию приобретает тот, кто проводил переустановку.

Следует учитывать и возможность пользования чужим именем и паролем. В данном варианте необходимо не только проводить соответствующий инструктаж сотрудников, но и вводить систему регулярной (не реже чем в 2–3 месяца) смены паролей, а также программное обеспечение на местах настраивать таким образом, что если исполнитель вошел в систему под своим именем, но отсутствует на рабочем месте, то компьютер блокируется и ожидает заново ввода соответствующего пароля.

Ограничение права доступа в помещение, оборудование этих помещений и операции с секретной информацией достаточно полно регулируются инструкциями по защите секретной информации, и в данном случае нет необходимости их дублировать. К этим инструкциям хотелось бы добавить ряд рекомендаций по усилению данных мер, зачастую облегчающих соблюдение режимных требований.

Одной из основных проблем является учет магнитных носителей и запись на них. Передвижение магнитных носителей и кто и что записывает на них в условиях производства очень трудно учесть. Но наличие качественной компьютерной сети на предприятии исключает движение магнитных носителей между отделами. А изъятие дисководов гибких дисков из всех производственных компьютеров делает невозможным копирование информации на самый массовый носитель — гибкие диски, дискеты. Далее, запись на ленту наиболее технологично располагать на сервере, а сервер, как сказано выше, должен находиться в специальном помещении с ограниченным доступом, следовательно, в данном случае требования режима соблюдаются. Остается устройство записи на компакт-диск. Это основной способ вывода результата и хранения. В данном случае наиболее целесообразно иметь отдельный компьютер, соединенный в общую сеть, который может находиться в регистратуре или спецчасти предприятия. В таком случае запись готовой продукции на магнитные носители будет происходить максимально близко к режимным требованиям. А проследить, что именно записывается на носитель и кем, не представит труда, да и в большинстве случаев носители не будут покидать пределов регистратуры и спецчасти, так как при необходимости ввести в производство хранимую информацию можно прямо через тот же компьютер.

Если к описанному выше добавить меры по защите от несанкционированного вскрытия системных блоков компьютеров, то в результате мы получаем, что:

— в производственных помещениях полностью отсутствует перемещение магнитных носителей с режимной информацией, остаются только магнитные носители с программным обеспечением;

— отсутствует возможность выполнить какое-либо несанкционированное копирование информации с рабочих мест.

Незащищенными остаются: устройства вывода на печать, их результаты и работа с материалами по сканированию.

RESUME

Recommendations and the basic principles are given on streaming and protection of the production information for the projects aimed at digital mapping and creation of land use information systems.