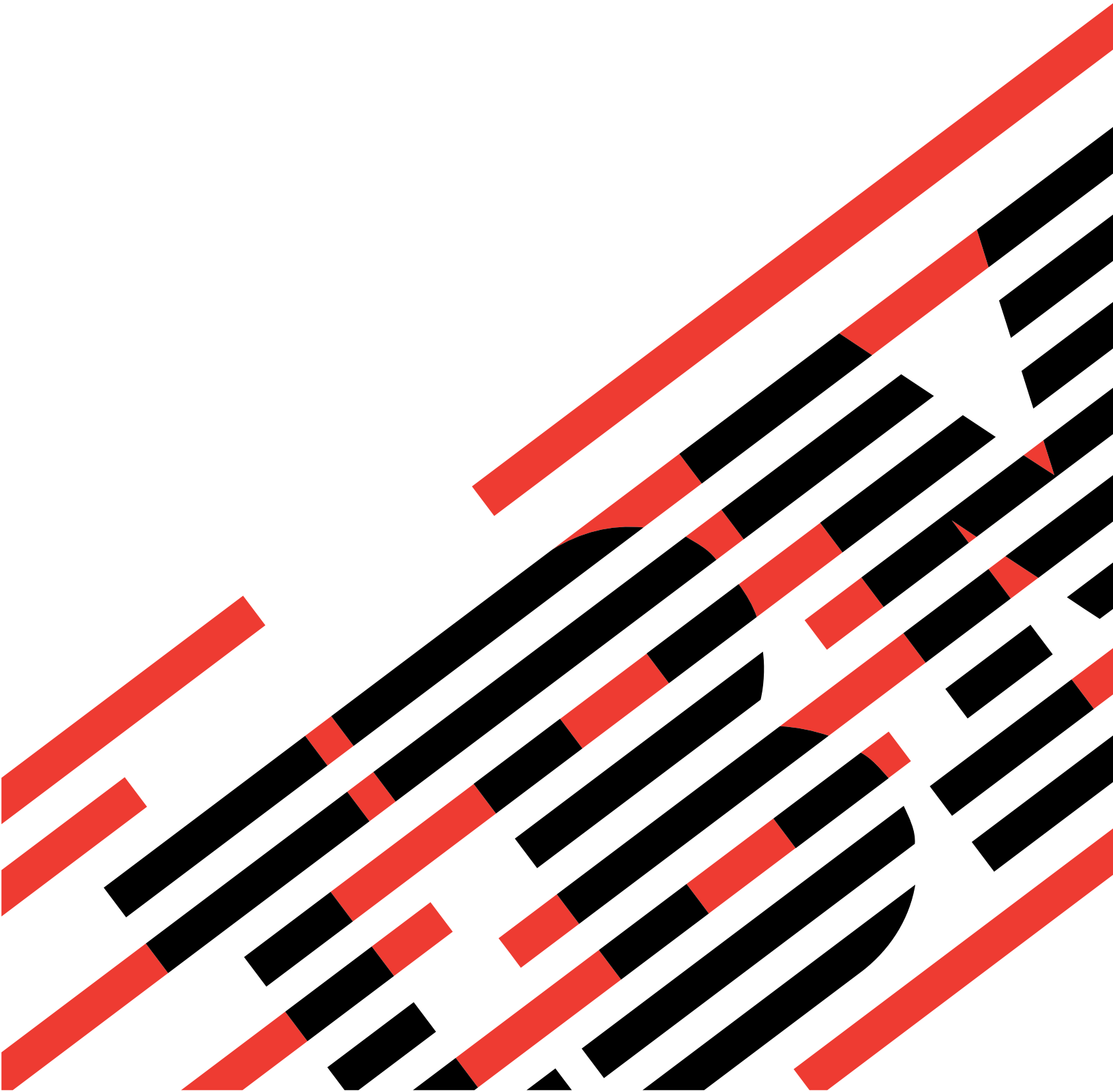
IBM

eserver

iSeries

Основные принципы защиты системы

Версия 5, выпуск 3



IBM

@server

iSeries

Основные принципы защиты системы

Версия 5, выпуск 3

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 137.

Пятое издание (август 2005 г.)

Это издание относится к версии 5, выпуску 3, модификации 0 IBM Operating System/400 (код продукта 5722-SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

Содержание

Основные принципы защиты системы

В этой книге приведена подробная информация по планированию и настройке защиты iSeries. Особое внимание уделено процедурам планирования - в этом разделе вы найдете бланки, которые помогут вам разработать план защиты системы. Кроме того, вы можете ознакомиться с подробным описанием процедур настройки средств защиты в системе. В связи с тем, что данная информация предназначена для использования в качестве справочника по настройке, мы рекомендуем напечатать ее.

Установка системы защиты iSeries делится на два больших этапа: этап планирования и этап настройки. Для того чтобы правильно организовать защиту системы, прочитайте следующие разделы:

- Защита системы - Введение: включает обзор принципов защиты и содержит ответы на вопросы об основах защиты системы.
- Защита для пользователей - Планирование: описывает планирование аспектов защиты, влияющих на работу пользователей в системе. В разделе рассматривается физическая защита, защита приложений, общая стратегия защиты и организация профайлов пользователей в системе.
- Защита ресурсов - Планирование: включает информацию о планировании защиты системных объектов, включая библиотеки и хранящиеся в них объекты, а также принтеры, вывод принтеров и рабочие станции.

После того, как вы завершили планирование, вы можете просмотреть следующие разделы, посвященные настройке защиты:

- Защита для пользователей - Настройка: включает подробное описание настройки защиты для пользователей и групп.
- Защита ресурсов - Настройка: содержит инструкции по установке принадлежности объектов, общих и специальных прав доступа к объектам, а также сведения о защите рабочих станций и принтеров.
- Тестирование защиты: рассказывает о том, как проверить правильность настройки защиты в системе.
- Изменение информации о защите: описывает изменение профайлов пользователей и групп, а также обновление параметров защиты ресурсов.
- Сохранение информации о защите: рассматривает вопросы резервного копирования и восстановления данных защиты.
- Контроль защиты: включает справочные таблицы для слежения за работой системы защиты и информацию о средствах контроля.

Кроме этого, в книге присутствуют формы планирования, которые помогут вам разработать стратегию защиты и задать конфигурацию системы.

Как напечатать этот раздел

Вы можете загрузить этот документ в формате PDF для последующего просмотра или печати. Для просмотра файлов в формате PDF необходима программа Adobe® Acrobat® Reader. Ее можно загрузить с Web-сайта Adobe  .

Для просмотра или загрузки этого документа в формате PDF выберите ссылку Защита системы (около 950 Кб, 164 страницы).

Для сохранения соответствующего файла выполните следующие действия:

1. Откройте файл в браузере (для этого щелкните на предыдущей ссылке).
2. Выберите в окне браузера меню **Файл**.
3. Выберите пункт **Сохранить как...**
4. Выберите каталог для сохранения файла.

5. Нажмите кнопку **Сохранить**.

Защита системы - Введение

Вопросы защиты важны для всех сотрудников компании, работающих с системой, начиная от обычных пользователей, и заканчивая системными администраторами. Под защитой системы понимается как защита самого сервера iSeries, так и защита конфиденциальной и деловой информации от преднамеренного или случайного искажения или копирования.

Вы можете настроить параметры защиты системы в соответствии с конкретными требованиями, предъявляемыми в вашей организации.

Средства защиты можно рассматривать как своеобразную дверь для входа в систему. Вы можете **запереть** дверь, т.е. защитить информацию от несанкционированного доступа.

Кроме того, вы можете **открыть** для отдельных пользователей те или иные возможности системы.

Следует помнить, что хорошая стратегия защиты поможет защитить вашу систему, но никакая стратегия не может гарантировать сохранность оборудования и информации. Рекомендуется разделить права доступа к системе между несколькими пользователями, чтобы ни один из них не обладал полным контролем над системой.

В этой книге приведены подробные пошаговые инструкции, которые помогут вам при планировании и настройке защиты. В этом разделе проиллюстрирована важность планирования защиты и приведены формы планирования, в которых вы сможете записывать свои решения, относящиеся к принципам защиты системы. Кроме того, в этом разделе приведен пример настройки защиты для вымышленной компании JKL Toys.

Настройку защиты следует начинать с тщательного предварительного планирования. Основные требования защиты и важность планирования описаны в следующих разделах:

- Часто задаваемые вопросы о защите системы
- Защита системы - Обзор
- Планирование защиты системы

Для полной защиты системы необходимо также разработать стратегию сохранения и восстановления всей информации. Кроме того, необходим план по замене оборудования в случае стихийного бедствия. Дополнительная информация по этим вопросам приведена в разделе Information Center Резервное копирование и восстановление.

Защита пользователей

Планирование защиты пользователей описано в следующих разделах:

- Планирование защиты приложений
- Планирование стратегии защиты
- Планирование групп пользователей
- Планирование профайлов пользователей

Защита ресурсов

Планирование защиты ресурсов описано в следующих разделах:

- Основные сведения о типах прав доступа
- Планирование защиты библиотек приложений
- Выбор владельца для библиотек и объектов
- Объединение объектов в группы
- Защита вывода на принтер

- Защита рабочих станций
- Планирование установки приложений

Формы планирования

В этой книге приведены формы планирования, которые вы можете напечатать и записывать в них все свои решения, связанные с защитой. Вы можете загрузить этот раздел в формате PDF и напечатать его целиком или только отдельные формы планирования.

Настройка защиты

В этом разделе приведены инструкции, которые помогут вам реализовать выбранную стратегию защиты. Настройка защиты системы описана в следующих разделах:
- Настройка защиты пользователей
- Настройка защиты ресурсов

Часто задаваемые вопросы о защите системы

В этом разделе приведен список часто задаваемых вопросов о защите системы, а также даны ответы на эти вопросы, которые помогут вам лучше понять важность организации защиты.

Почему защита так важна?

Хранящаяся в системе информация - это одна из важнейших составляющих вашего бизнеса. При планировании необходимо помнить, что готовая система защиты должна обеспечивать следующие свойства информации:
- **Конфиденциальность:** предотвращение несанкционированного просмотра и копирования информации.
- **Целостность:** предотвращение несанкционированного изменения (искажения) или удаления информации.
- **Доступность:** защита от случайного или преднамеренного повреждения информации.

Обычно люди воспринимают защиту системы как защиту от посторонних лиц, не работающих в данной организации, например, от конкурентов. На самом же деле, хорошо настроенная защита чаще защищает от случайностей и не в меру любопытных пользователей из своей же организации. В системе без защиты любой пользователь может случайно удалить важный файл. Защита позволяет предотвратить ошибки такого рода.

Требуемый уровень защиты системы определяется ответами на следующие вопросы:
- Насколько важна для вашей фирмы защищаемая система и хранящаяся в ней информация?
- Предъявляются ли в вашей фирме специальные требования к защите?
- Предъявляются ли в вашей фирме специальные требования к защите электронной информации?
- Собираетесь ли вы в ближайшем будущем изменять общей уровень защиты?

Зачем нужно изменять конфигурацию системы?

Системы семейства iSeries предназначены для различных целей. В небольшой системе может быть всего лишь 3-5 пользователей, работающих с небольшим числом приложений. В крупных системах число пользователей может достигать нескольких тысяч; при этом может использоваться множество различных приложений.

Гибкие средства настройки системы iSeries позволяют применять ее в самых разных ситуациях. Вы можете изменять число пользователей и приложений, руководствуясь текущими требованиями.

Вам необязательно начинать настройку сразу после получения новой системы. Для многих параметров предусмотрены начальные значения или **значения по умолчанию**. Эти значения выбраны таким образом, что их можно применять в большинстве систем.

Примечание: Все новые системы поставляются с уровнем защиты **40**. При этом с системой могут работать только определенные в ней пользователи. Кроме того, этот уровень защиты предотвращает нарушения целостности данных выполняющимися в системе программами.

Однако, небольшая настройка может упростить работу с системой и сделать ее более эффективной. Например, вы можете сделать так, чтобы каждый пользователь после входа в систему видел нужное ему меню. Отчеты пользователей могут автоматически отправляться на тот или иной принтер. Пользователи будут чувствовать себя увереннее при работе с системой, если она будет настроена в соответствии с их требованиями.

Кто должен отвечать за защиту?

Разные компании по разному подходят к решению этого вопроса. Иногда за все аспекты защиты отвечает программист. В других случаях это может быть администратор системы. Если вы не уверены, какое их этих решений следует выбрать, то рекомендуется следующий подход:

- Планирование защиты ресурсов зависит от того, приобретает ваша компания приложения или разрабатывает их самостоятельно. При самостоятельной разработке приложений требования защиты должны учитываться уже в процессе проектирования. Если вы приобретаете приложения, то проконсультируйтесь с их разработчиком. В любом случае, требования защиты обязательно должны учитываться в процессе разработки приложения.
- Настройка защиты должна входить в круг обязанностей системного администратора. Именно администратор системы определяет пользователей и их права доступа. Кроме того, системный администратор может выполнять другие процедуры, такие как сохранение и восстановление информации.
- Настройкой самой системы также должен заниматься администратор, поскольку параметры защиты часто связаны с прочими параметрами системы.

Независимо от того, кто отвечает за защиту, **доведите требования защиты до всех сотрудников**. Уведомите всех, желательно письменно, о том, что хранящаяся в системе информация - это важная часть собственности компании. Информация должна защищаться наравне с любой другой собственностью. Пример стратегии защиты приведен в разделе ″Пример стратегии защиты компании JKL Toys″.

Теперь вы можете перейти к обзору средств защиты системы.

Защита системы: Обзор

Планирование защиты будет эффективным только при условии, что вы понимаете, насколько ваше представление о том, что вы хотите делать, соответствует возможностям системы. Для достижения цели вам нужно представлять, как взаимодействуют пользовательские и системные функции.

В перечисленных ниже разделах приводится общая информация о различных аспектах защиты и настройки и показано, как они сочетаются друг с другом. Ознакомьтесь с ними, перед тем как начинать планирование. Основные положения, изложенные в этих разделах, подробно объясняются по мере необходимости в процессе планирования.

- Встроенная системная защита
- Основные термины
- Защита с точки зрения пользователя
- Системные средства для защиты и настройки

Встроенная системная защита

Все средства системной защиты встроены в операционную систему. Они не продаются в виде отдельного продукта. Такой комплексный подход обладает определенными преимуществами:

- Система защиты полностью согласована с операционной системой. Для ее настройки используются те же меню, команды и термины.

- Пользователи не могут обойти окна защиты, так как она является неотделимой частью программного обеспечения.
- Правильно построенная защита оказывает минимальное воздействие на производительность системы.
- С развитием программных средств развивается и защита. Версии программного продукта с новыми функциями содержат и средства защиты для этих функций.

Системы iSeries поставляются с уровнем защиты 40, на котором незарегистрированные пользователи не могут входить в систему и, кроме того, сведен к минимуму риск возможного нарушения целостности данных со стороны программ, которые могут обойти защиту. Однако вы можете и сами задавать определенные параметры защиты или изменять ее уровни. Уровни защиты описываются в разделе ″Выбор уровня защиты″.

Ознакомившись с тем, как работает встроенная системная защита, вы можете перейти к изучению общей терминологии системы iSeries.

Основные термины

Для понимания принципов работы системы iSeries необходимо освоить следующий набор основных терминов:

Объект

Объект - это именованная область, которой можно управлять. Наиболее часто встречающиеся объекты - это файлы и программы. Другие типы объектов - команды, очереди, библиотеки и папки. Объект в системе определяется именем, типом и библиотекой, в которой он находится. Для любого объекта в системе можно установить защиту.

Библиотека

Библиотека - это специальный тип объекта, предназначенный для объединения других объектов. В библиотеках хранятся многие объекты системы.

Каталог

Каталог - это еще один способ объединения объектов в системе. Объекты могут храниться в каталоге. Каталог может содержать другой каталог; таким образом формируется иерархическая структура.

Ознакомившись с основными терминами, применяемыми при описании системы iSeries, вы можете посмотреть на защиту с точки зрения пользователя.

Защита с точки зрения пользователя

С точки зрения пользователя, защита определяет, какие задачи пользователь может выполнять в системе и каким образом, а также способ взаимодействия пользователя с системой при выполнении этих задач. Вопрос о том, как защита будет влиять на работу пользователей, требует тщательного обдумывания. Например, если установить срок действия паролей равным пяти дням, то это может мешать пользователям выполнять свои задачи. С другой стороны, слишком либеральная политика в отношении паролей может привести к проблемам с безопасностью системы.

Для того чтобы обеспечить надежную защиту вашей системы, защиту необходимо подразделить на отдельные категории, которые можно планировать, которыми можно управлять и за которыми можно наблюдать. С точки зрения пользователя, защита системы может быть подразделена на несколько частей:

Физический доступ к системе

Под физической защитой подразумевается защита системного блока, всех системных устройств и носителей резервных копий, таких как дискеты, магнитные ленты и компакт-диски, от случайного или намеренного повреждения или утери.

Большинство предпринимаемых вами мер по физической защите системы являются внешними по отношению к ней. Вместе с тем, в комплект поставки системы входит замок или электронный ключ, который позволяет установить запрет на несанкционированное использование функций на системном блоке.

Подробная информация о планировании физической защиты системы приведена в разделе ″Планирование физической защиты″.

Порядок входа пользователей в систему

Защита при входе в систему позволяет предотвратить работу в системе незарегистрированных в ней пользователей. Для того чтобы войти в систему, пользователь должен ввести правильный идентификатор и пароль.

Полностью предотвратить возможные нарушения защиты вашей системы можно как с помощью задания соответствующих системных параметров, так и с помощью настройки пользовательских профайлов. Например, вы можете потребовать, чтобы пароли регулярно сменялись. Можно также запретить использование паролей, которые легко угадать.

Набор действий, разрешенных пользователям

Важная роль защиты, так же как и настройки системы, заключается в определении круга задач, которые разрешено выполнять пользователю. При этом защита выполняет **запретительную** функцию, например, запрещает некоторым пользователям просматривать определенную информацию, тогда как настройка системы выполняет **разрешительную** функцию. В системе, настроенной правильно, пользователям предоставлена возможность эффективно выполнять свои задания, поскольку доступ к ненужным задачам и информация исключен.

Часть того, что могут делать пользователи, определяется системным администратором, а часть - разработчиком программы. Приведенная здесь информация касается главным образом тех функций, которые обычно выполняются системным администратором. Описания всех системных значений вы можете найти в главе 3, ″Security System Values,″ книги *Security-Reference*(SC41-5302)  .

Параметры, определяющие действия, которые пользователю разрешено выполнять в системе, задаются в пользовательском профайле, описаниях заданий и классах. Их описание приведено ниже:

Разрешение выполнять только определенные функции
: Вы можете ограничить возможности пользователя, разрешив ему доступ только к конкретной программе, меню или набору меню и к нескольким системным командам. Эти ограничения устанавливаются в профайле пользователя. Как правило, профайлы пользователей создаются и контролируются системным администратором.

Запрет на выполнение системных функций
: Системные функции позволяют сохранять и восстанавливать информацию, управлять выводом на принтер и определять новых пользователей. В профайле пользователя определяется, какие из наиболее употребительных системных функций разрешено выполнять этому пользователю.

  В системе iSeries обращение к системным функциям осуществляется с помощью команд управляющего языка (CL) и интерфейсов прикладных программ (API). И команды, и интерфейсы представляют собой объекты. Поэтому для определения того, кому именно разрешено выполнять эти команды и системные функции, можно использовать понятие прав доступа к объектам.

Определение пользователей, которым разрешено обращаться к файлам и программам
: Защита ресурсов позволяет управлять доступом к объектам в системе. Для любого объекта вы можете указать, кому и как разрешено работать с этим объектом. Например, одному пользователю вы можете разрешить только чтение файла, другому - изменение файла, третьему - изменение и удаление файла.

Предотвращение нерационального использования системных ресурсов

Для вас может иметь значение не только сохранность данных в вашей системе, но и производительность системы. Системный администратор может контролировать правильность использования ресурсов: например, устанавливать приоритет выполнения пользовательских заданий, очередность печати или ограничения на объем доступного дискового пространства.

Обмен информацией с другими компьютерами

Если ваша система соединена с другими компьютерами или с программируемыми рабочими станциями, необходимо принять дополнительные меры по ее защите. В противном случае пользователь с другого компьютера в сети сможет запускать задания или обращаться к информации на вашем компьютере, не входя в систему.

Вы можете управлять запуском удаленных заданий и удаленным доступом к данным и к компьютерам с помощью системных значений и сетевых атрибутов. Если вы разрешаете удаленный доступ, то вы можете указать, какую защиту при этом следует применять. Описания всех системных значений вы можете найти в главе 3, ″Security System Values,″ книги *Security-Reference*(SC41-5302). 

Сохранение информации о защите

Необходимо регулярно выполнять резервное копирование информации в вашей системе. Необходимо сохранять не только данные, но и информацию о защите. Помните, что в случае аварии вам нужно будет восстанавливать информацию о пользователях, информацию о правах доступа и сами данные.

Процедура сохранения информации о защите описана в разделе ″Сохранение информации о защите″. Более подробные сведения о создании резервных копий и восстановлении информации о защите приведены в разделе Резервное копирование и восстановление Information Center.

Контроль защиты

В системе предусмотрено несколько способов контроля эффективности защиты:

- Сообщения, отправляемые системному оператору при обнаружении определенных нарушений защиты.
- Ведение специального журнала контроля, в который заносятся транзакции, приводящие к нарушению защиты.

Общие сведения о применении этих средств приведены в разделе ″Контроль защиты″. Дополнительную информацию можно найти в главе 9, ″Auditing Security on the System,″ книги *Security-Reference* (SC41-5302).

Для более полного понимания принципов настройки вашей системы ознакомьтесь с разделом, в котором настройка системы рассматривается с точки зрения пользователя.

Настройка системы с точки зрения пользователя: Вы можете настроить систему так, чтобы пользователям было удобно работать. Для этого подумайте, что именно нужно пользователям для успешного выполнения задач. Определить, какие меню и приложения должны быть ″видны″ пользователю, можно несколькими способами:

Выдача пользователям информации, которую они хотят видеть

Большинство из нас организует свой рабочий стол или офис таким образом, чтобы наиболее доступными были самые необходимые предметы. Рассмотрите с этой точки зрения доступ пользователей к системе. После того, как пользователь войдет в систему, он должен увидеть меню или окно, с которыми он наиболее часто работает. Реализацию этой функции можно легко предусмотреть в пользовательском профайле.

Ограничение доступа к ненужной информации

В системе, как правило, существует множество различных приложений. Большинству пользователей необходимо видеть только те приложения, которые нужны им для выполнения своих заданий. Ограничьте доступ пользователей к системе несколькими функциями, которые упрощают выполнение заданий. Это можно сделать с помощью пользовательских профайлов, описаний заданий и соответствующих меню.

Правильная организация обработки вывода

Пользователи не должны беспокоиться о том, как отправить отчет на нужный принтер или как должны выполняться их пакетные задания. Эти процедуры определяются системными значениями, пользовательским профайлом и описаниями заданий.

Обеспечение операционной поддержки

Независимо от того, насколько хорошо вы настроили систему, пользователи могут задавать вопросы типа ″Где находится мой отчет?″ или ″Мое задание еще не запущено?″. Простой интерфейс с системными функциями, позволяющий отвечать на такие вопросы пользователей, обеспечивает меню **Операционная поддержка**. В зависимости от квалификации пользователей, существуют различные варианты системных меню, называемые **уровнями поддержки**. Поставляемая система настроена таким образом, что меню Операционная поддержка автоматически доступны всем пользователям. Однако формат ваших приложений может потребовать, чтобы вы изменили способ получения пользователями доступа к меню Операционная поддержка.

В системе iSeries предусмотрены служебные программы, позволяющие защитить ресурсы, не ограничивая доступа пользователей к ним.

Системные средства для защиты и настройки

Планирование защиты будет эффективным только при условии, что вы понимаете, насколько ваше представление о защите соответствует возможностям системных средств. Вы можете применять эти средства для настройки защиты в вашей системе.

Уровень защиты

Все новые системы iSeries поставляются с уровнем защиты 40. Уровень 40 обеспечивает защиту паролем, защиту ресурсов и целостность системы. Если вы хотите изменить действующий в системе уровень защиты, измените системное значение QSECURITY. Однако фирма IBM настоятельно рекомендует оставить уровень защиты 40. Уровень защиты может быть изменен пользователем, принадлежащим классу *SECOFR или обладающим специальными правами доступа *ALLOBJ и *SECADM.

В таблице представлены четыре уровня защиты, предоставляемые системой:

Таблица 1. Возможные уровни защиты в системе

Уровень защиты	Описание
Уровень защиты 20	Только защита паролем.
Уровень защиты 30	Защита паролем и защита ресурсов.
Уровень защиты 40	Защита паролем, защита ресурсов и защита целостности данных.
Уровень защиты 50	Защита паролем, защита ресурсов и расширенная защита целостности данных.

Информация о том, как выбрать нужный вам уровень защиты, приведена в разделе ″Выбор уровня защиты″.

Системные значения

Вы можете изменять системные значения, управляя работой различных функций iSeries. Системные значения определяют стратегию защиты на уровне компании. Системные значения одинаковы для всех пользователей системы, за исключением тех случаев, когда они переопределяются явным образом (например, профайлом пользователя).

Системные значения определяют, например, главный принтер, формат выдачи дат и срок действия пароля.

Сетевые атрибуты

Сетевые атрибуты определяют, каким образом система соединяется с другими компьютерами, в том числе персональными. Сетевые атрибуты относятся ко всей системе целиком.

Профайлы групп

Профайл группы определяет группу пользователей. Он определяет стратегию защиты на уровне отдела. Профайлы групп могут использоваться как шаблоны для создания профайлов отдельных пользователей. Кроме того, с помощью профайлов групп можно определять права доступа членов группы к объектам в системе. Дополнительная информация о профайлах групп приведена в разделе ″Планирование групп пользователей.″

Профайлы пользователей

Профайл пользователя - это один из наиболее мощных и гибких инструментов настройки. В профайле пользователя задается пароль пользователя и определяется меню, которое пользователь видит после входа в систему. Профайл пользователя определяет, какие действия разрешены пользователю, а какие - запрещены. Он задает вид системы с точки зрения пользователя. Советы по планированию профайлов пользователей приведены в разделе ″Планирование: защита для пользователей″.

Описания заданий

Описание заданий в сочетании с системными значениями и профайлами пользователей определяет, каким образом система обрабатывает задания пользователя. Описание задания устанавливает начальный список библиотек, который определяет, к каким библиотекам пользователь автоматически получает доступ после входа в систему.

Защита ресурсов

Для того чтобы защитить ресурсы (объекты) в системе, системный администратор определяет, кто и как может работать с ними. Системный администратор может задавать права доступа как к отдельным объектам, так и к группам объектов (т.н. списки прав доступа). Как правило, защита устанавливается для файлов, программ и библиотек, но система позволяет устанавливать права доступа к любым объектам.

Управлять защитой ресурсов можно достаточно просто и эффективно, если заранее сформулировать основные принципы ее построения. Схема защиты ресурсов, созданная без предварительного плана, может оказаться сложной и неэффективной. Способы планирования защиты ресурсов описаны в разделе ″Планирование защиты для ресурсов″.

В системе предусмотрено несколько средств, позволяющих реализовать простую схему защиты ресурсов:

- **Профайлы групп:** Одинаковых пользователей можно объединять в группу с одним и тем же профайлом группы. Всем пользователям в группе предоставляются одинаковые права доступа к объектам.
- **Списки прав доступа:** Объекты, требующие одинаковой защиты, можно объединять в один список. При этом вы можете предоставлять права доступа не к отдельному объекту, а ко всему списку.
- **Принадлежность объекта:** Каждый объект в системе имеет владельца. Владельцем объекта может быть профайл группы или отдельный пользователь. Правильный выбор владельца объекта позволяет: (1) управлять приложениями и (2) передавать полномочия по защите информации.

- **Основная группа:** Для объекта можно задавать права доступа основной группы. Система хранит права доступа основной группы вместе с объектом. Применение основной группы позволяет упростить управление правами доступа и усовершенствовать процедуру проверки прав доступа.
- **Права доступа к библиотеке:** Файлы и программы, требующие защиты, можно помещать в библиотеку и задавать права доступа к этой библиотеке. Часто это гораздо проще, чем ограничивать доступ к каждому объекту по отдельности. В случае особо важных объектов можно устанавливать защиту и для объекта, и для библиотеки.
- **Права доступа к объекту:** В тех случаях, когда недостаточно ограничить доступ к библиотеке, можно ограничить доступ к отдельным объектам, например, файлам.
- **Общие права доступа:** Это права доступа, предоставляемые пользователю, у которого нет частных прав доступа к объекту, который не содержится в списке прав доступа к объекту и группе которого не выделены специальные права доступа к объекту. Общие права доступа позволяют эффективно защищать объекты, не содержащие конфиденциальной информации, и обеспечивать высокую производительность системы.
- **Права доступа к каталогу:** Права доступа к каталогу можно использовать точно так же, как и права доступа к библиотеке. Объекты можно объединить в каталог и защищать не каждый объект в отдельности, а сразу все объекты в этом каталоге.
- **Владелец прав доступа:** При удалении объекта удаляется информация о правах доступа к этому объекту. Если приложение удаляет и затем вновь создает описанные в программе файлы, то информация о правах доступа к этим файлам сохраняется во владельце прав доступа. Владельцы прав доступа могут быть полезны при переходе от системы System/36.

Средства защиты

С помощью средств защиты вы можете управлять параметрами защиты системы iSeries. В этих же целях вы можете применять и профайлы пользователей:

- Выясните, какие профайлы пользователей имеют пароли по умолчанию.
- Запланируйте время дня и дни недели, когда профайлы пользователей будут недоступны.
- Запланируйте удаление профайла пользователя в случае увольнения сотрудника.
- Выясните, какие профайлы пользователей имеют специальные права доступа.
- Выясните, кому предоставляются права доступа к объектам в системе.

С помощью средств защиты можно отслеживать общие и частные права доступа, связанные с конфиденциальными (секретными) объектами. Вы можете регулярно (например, ежемесячно) печатать эти отчеты, чтобы выяснить, на каком именно участке защиты нужно сконцентрировать свое внимание. Вы можете настроить процедуру создания этих отчетов таким образом, чтобы в них отражались только те изменения, которые произошли после получения предыдущего отчета.

Существуют и другие средства, позволяющие следить за действиями в системе:

- Программы триггера
- Параметры защиты, задаваемые в записях средств связи, описаниях подсистем, очередях вывода, очередях заданий и описаниях заданий.
- Случайно или намеренно изменяемые программы

Теперь, когда вы понимаете всю важность защиты системы, вы можете ознакомиться с описанием способа планирования, приведенного в этом разделе в качестве примера.

Планирование защиты системы

Защиту системы следует планировать путем перехода от общего к частному и от внешних атрибутов к внутренним. Например, при планировании пользовательских профайлов сначала необходимо решить, какие объекты должны быть доступны тому или иному пользователю (внешний атрибут), и только потом выбирать способ реализации (внутренний атрибут). Аналогично, сначала нужно спланировать системные значения и профайлы групп (общие объекты), а затем описать исключения для конкретных пользователей

(частные объекты). Действия по планированию, описанные в разделе Планирование защиты пользователей следует выполнять строго по порядку. В этом разделе подробно описаны процедуры планирования режима работы и защиты системы.

Защита системы планируется и реализуется постепенно. Сначала принимаются решения по наиболее общим вопросам, а затем рассматриваются более глубокие и сложные вопросы защиты. Начните с физической защиты системы, а затем перейдите к защите приложений и настройке системных значений. После этого можно перейти к настройке параметров защиты для конкретных пользователей и объектов.

Во всех разделах, связанных с планированием, этот подход иллюстрируется на примере компании JKL Toys. Раздел ″Компания JKL Toy: Знакомство″ описывает эту гипотетическую компанию, используемую в примерах.

В разделе ″Инструкции по планированию″ вы найдете краткое описание каждого шага узнаете о взаимосвязи различных шагов.

Компания JKL Toys

Примеры упрощают как объяснение, так и понимание. В качестве примера в данной книге выбрана компания JKL Toys. JKL Toys - это небольшая, но быстро растущая компания по производству игрушек, перед которой возникла задача настройки защиты системы iSeries. Президент компании Джон Смит надеется, что новая система iSeries упростит управление быстро растущим предприятием.

Джон назначил системным администратором Шэрон Джонс, главного бухгалтера компании. Шэрон понимает важность планирования и хочет как можно более тщательно спланировать установку и настройку системы. Сейчас компания невелика, поэтому, за некоторыми исключениями, ее сотрудникам необходим доступ ко всей информации. Однако по мере роста компании это положение должно измениться. Шэрон хочет сразу организовать такую стратегию защиты, чтобы упростить изменение настройки в дальнейшем.

Компания JKL Toys планирует применять следующие приложения: Заказы клиентов, Управление запасами, Контракты и цены, Дебиторская задолженность. В разделах, посвященных планированию, приведена дополнительная информация о стратегии защиты, реализуемой в компании JKL Toys.

Процедуры планирования защиты описаны в разделе ″Инструкции по планированию″.

Инструкции по планированию защиты

В следующей таблице описаны все операции планирования и приведены сведения о взаимосвязи этих операций:

Таблица 2. Инструкции по планированию защиты

Этап	Цель	Связанные действия
Планирование физической защиты	Планирование защиты системного блока, устройств и носителей с резервными копиями информации	Это сравнительно самостоятельная операция. Информация о физической защите не вводится в систему, но может влиять на планирование системных значений и параметры защиты ресурсов.
Планирование установки приложений	Описание функций, главных меню и библиотек всех приложений системы.	Информация применяется на всех остальных этапах планирования и настройки защиты. Эта информация не вводится в систему.
Планирование общей стратегии защиты	Определение общего подхода к вопросам защиты. Выбор соответствующих системных значений.	Применяется информация, созданная при планировании установки приложений. Выбранные системные значения влияют на планирование пользователей и групп.

Таблица 2. Инструкции по планированию защиты (продолжение)

Этап	Цель	Связанные действия
Планирование групп пользователей	Объединение пользователей в группы. Определение характеристик каждой группы.	Применяется информация, созданная при планировании установки приложений. Группы пользователей влияют на планирование отдельных пользователей.
Планирование профайлов пользователей	Выбор группы для каждого пользователя системы. Определение характеристик каждого пользователя, отличных от характеристик группы. Например, пользователь может отличаться от своей группы доступом к определенным приложениями или библиотекам.	Применяется информация, созданная при планировании приложений и групп пользователей.
Планирование защиты ресурсов	Определение общедоступных приложений. Ограничение доступа пользователей к приложениям.	Применяется информация, созданная при планировании приложений и групп пользователей.
Планирование установки приложений	Определение владельцев и прав доступа к библиотекам приложений.	Применяется информация, собранная при планировании защиты ресурсов.

Начните процесс планирования защиты с раздела Планирование защиты пользователей.

Планирование защиты пользователей

Планирование защиты пользователей включает все вопросы взаимодействия пользователей со средствами защитой системы. Необходимо обратить внимание на следующие аспекты защиты:

Физическая защита

Под физической защитой понимается защита самого сервера iSeries от случайного или преднамеренного повреждения, либо кражи. Кроме того, физическая защита предусматривает ограничение доступа к рабочим станциям, принтерам и носителям информации. Дополнительная информация о планировании физической защиты, возможных рисках и рекомендациях фирмы IBM приведена в разделе ″Планирование физической защиты″.

Защита приложений

Разработка защиты приложений включает выбор приложений, которые должны быть установлены в системе, а также собственно защиту этих приложений с одновременным предоставлением пользователям доступа к ним. Более подробная информация о приложениях приведена в разделе ″Планирование защиты приложений″.

Общая стратегия защиты

Под планированием общей стратегии защиты понимается разработка такого плана защиты, который учитывает как текущие требования компании, так и требования, которые могут возникнуть в дальнейшем в результате развития бизнеса. Дополнительная информация о выборе стратегии защиты, уровня защиты, паролей и системных значений приведена в разделе ″Планирование общей стратегии защиты″.

Защита групп пользователей

Группа - это объединение пользователей, которым необходимы одинаковые права доступа к одним и тем же приложениям. Планирование групп пользователей включает определение состава каждой группы и набора приложений, которые должны быть доступны пользователям этой группы. Более подробная информация о планировании групп пользователей и профайлов групп, а также о выборе системных значений приведена в разделе ″Планирование групп пользователей″.

Защита отдельных пользователей

После определения будущих групп пользователей можно перейти к планированию отдельных

пользовательских профайлов. Дополнительная информация о выборе имен и прав доступа пользователей, а также о настройке системных значений приведена в разделе ″Планирование профайлов пользователей″.

Все эти разделы содержат ссылки на формы планирования, которые вы можете напечатать и записывать в них свои решения по настройке защиты.

Планирование физической защиты

Перед установкой системы iSeries создайте план ее физической защиты. Для этого ответьте на следующие вопросы:

- Где будет размещаться системный блок?
- Где будут размещаться дисплейные станции?
- Где будут размещаться принтеры?
- Какое потребуется дополнительное оборудование, например, линии передачи данных, телефонные линии, мебель и сейфы?
- Какие меры будут предприняты против аварий, таких как пожар или сбой питания?

Физическая защита должна быть частью общей стратегии защиты. Конкретные действия по физической защите зависят от того, где будет размещена система и подключенные к ней устройства.

Записывайте решения по физической защите системы в форму Планирование физической защиты. Различные аспекты физической защиты обсуждаются в следующих разделах:

- Физическая защита системного блока.
- Физическая защита документации по системе и носителей с резервными копиями.
- Физическая защита рабочих станций.
- Физическая защита принтеров и вывода на принтер.
- Планирование стратегии защиты.

Каждый системный блок оснащен панелью управления для выполнения таких специальных операций, как включение и выключение системы. Для предотвращения несанкционированного доступа к панели управления предусмотрен электронный или механический замок. Этот замок может рассматриваться как дополнительное средство защиты, но он не должен заменять собой средства физической защиты.

Физическая защита системного блока

Для работы системы iSeries не требуется помещение со специальными условиями. Поэтому системный блок часто можно видеть установленным в центре офиса, где он оказывается доступным для большого числа людей. Заказчиков обычно привлекает небольшой размер и простота обслуживания системы iSeries, однако именно эти качества могут представлять угрозу безопасности системы. Например, установленный в общедоступном месте небольшой системный блок может быть украден.

Поместите системный блок в безопасном месте. Лучше, если он будет находиться в запертой комнате. По крайней мере, эта комната должна запираться в нерабочее время.

От чего следует защищать системный блок

Кроме уже упомянутой кражи, существует ряд других ситуаций, которые могут возникнуть в случае неправильной реализации или отсутствия физической защиты системы:

Случайное нарушение работы системы

Очень часто причиной нарушения защиты становятся не посторонние лица, а сами пользователи системы. Представьте, что одна из дисплейных станций системы зависла. Системный оператор отсутствует. Расстроенный пользователь идет к системному блоку и, не видя другого выхода, нажимает самую большую кнопку, искренне веря, что это поможет исправить положение. На самом деле эта кнопка выключает или перезагружает систему, в которой в это момент может работать

множество других заданий. После этого вам придется потратить не один час, восстанавливая частично обновленные файлы. Для предотвращения такой ситуации всегда запирайте панель управления на ключ.

Нарушение защиты с помощью DST

Защита системы не распространяется на функции DST, поскольку эти функции обычно применяются в особых ситуациях. В связи с этим пользователь, знающий или угадавший имя и пароль пользователя DST, может нанести существенный ущерб защите и самой системе. Более подробная информация о сервисных средствах приведена в разделе Специальные сервисные средства справочной системы Information Center.

Рекомендации

- Идеальным решением было бы размещение системного блока в запертой комнате. Если это невозможно, то необходимо, по крайней мере, ограничить доступ посторонних к системному блоку. Кроме того, желательно, чтобы системный блок находился в поле зрения ответственных сотрудников компании. Для предотвращения случайного или преднамеренного повреждения системы рекомендуется принять следующие меры:
- Блокируйте панель управления с помощью ключа (электронного или механического).
  - Для того чтобы систему можно было запустить без ключа, установите режим работы Normal.
  - Для применения функций автоматического управления питанием установите режим Auto.
  - Выньте ключ и поместите его в безопасное место.
- После установки системы и после работы обслуживающего персонала со Специальными сервисными средствами немедленно измените имя и пароль пользователя DST. Более подробные сведения приведены в разделе Специальные сервисные средства справочной системы Information Center.

В следующем разделе приведен пример защиты системного блока компании JKL Toys. Следующий этап - Физическая защита системной документации и носителей с резервными копиями.

Пример: Форма План физической защиты компании JKL Toys—Системный блок: Ниже приведен пример раздела формы План физической защиты, заполненной Шэрон Джонс для защиты системного блока, установленного в компании JKL Toys:

Таблица 3. Пример: Форма План физической защиты компании JKL Toys: Системный блок

План физической защиты	
Составлено: Шэрон Джонс	Дата: 9/2/99
Системный блок:	
Опишите меры защиты системного блока (например, запертая комната):	Системный блок расположен в комнате бухгалтерии. В дневную смену в комнате всегда находятся сотрудники бухгалтерии, которые могут следить за блоком. Сотрудники бухгалтерии также отвечают за кассу и важные записи. В нерабочие часы комната запирается.
Какое положение переключателя режима обычно используется?	Normal
Где хранится ключ?	В маленьком сейфе, расположенном в офисе Шэрон.
Другие сведения о системном блоке:	Системный блок легко доступен. Не забудьте предупредить сотрудников бухгалтерии о том, что они должны следить за появлением посторонних людей в комнате.

После разработки плана физической защиты системного блока вы можете перейти к планированию физической защиты системной документации и носителей информации.

Физическая защита системной документации и носителей с резервными копиями

План физической защиты системы должен включать защиту важной системной документации и носителей с резервными копиями информации. К системной документации относится информация, поставляемая фирмой IBM вместе с системой, пароли, формы планирования и отчеты, созданные системой.

В качестве носителей для хранения резервных копий могут применяться магнитные ленты, компакт-диски, дискеты и диски DVD. Одна копия системной документации и носителей с резервными копиями должна храниться в том же офисе, что и система, а другая - отдельно от системы. Эта информация потребуется для восстановления системы в случае повреждения или разрушения в результате стихийного бедствия. Ниже перечислены возможные варианты хранения системной документации и носителей с резервными копиями. Выберите наиболее подходящий вариант и запишите его в разделе Носители с резервными копиями и документация формы планирования Физическая защита.

Хранение системной документации

Пароли средств обслуживания и системного администратора необходимы для обеспечения правильной работы системы. Запишите их и сохраните в безопасном месте, доступ к которому ограничен. Сохраните копию этих паролей вне офиса вашей организации, чтобы можно было восстановить систему после аварии.

Рекомендуется также хранить отдельно прочую системную документацию, такую как параметры конфигурации и библиотеки основных приложений.

Хранение носителей с резервными копиями

После установки системы регулярно сохраняйте всю информацию на магнитную ленту или другой носитель. Эти резервные копии помогут вам восстановить систему в случае необходимости. Хранить их необходимо в безопасном месте, отдельно от системы.

Опасности

- Повреждение носителей с резервными копиями: если резервные копии будут повреждены в результате аварии или по каким-либо другим причинам, то при восстановлении системы вы сможете пользоваться только напечатанными отчетами.
- Кража носителей с резервными копиями или паролей: резервные копии могут содержать конфиденциальную информацию. В принципе, эта информация может быть восстановлена в другой системе.

Рекомендации

- Храните все пароли и носители с резервными копиями в пожаробезопасном закрытом помещении.
- Регулярно (например, раз в неделю) сохраняйте копию всей указанной информации в надежном месте, удаленном от основного сайта.

В следующем разделе приведен пример хранения документации в компании JKL Toys. Следующий этап - физическая защита рабочих станций.

Пример: Форма План физической защиты компании JKL Toys—Носители резервных копий и документация: Системный администратор компании JKL Toys Шэрон Джонс заполнила раздел формы План физической защиты, относящийся к внешним носителям информации и документации:

Таблица 4. Пример: Форма План физической защиты компании JKL Toys: носители резервных копий и документация

План физической защиты	
Составлено: Шэрон Джонс	Дата: 9/2/99
Носители резервных копий и документация:	

Таблица 4. Пример: Форма План физической защиты компании JKL Toys: носители резервных копий и документация (продолжение)

Где хранятся магнитные ленты с резервными копиями в офисе?	В большом несгораемом сейфе.
Где хранятся магнитные ленты с резервными копиями вне вашего офиса?	В несгораемом сейфе в офисе аудитора компании.
Где хранятся пароли администратора, SST и DST?	Вместе с кодом сейфа в офисе Джона Смита.
Где хранится важная системная документация, такая как серийные номера и информация о конфигурации?	В большом сейфе, расположенном вне офиса компании - в офисе аудитора.

По окончании планирования защиты носителей и документации вы можете перейти к планированию физической защиты рабочих станций.

Физическая защита рабочих станций

В большинстве случаев возможность входа пользователя в систему и его права доступа не зависят от рабочей станции. Однако, если некоторые рабочие станции находятся в общедоступных местах, то можете ограничить доступ к системе с этих станций. Кроме того, особого внимания требуют персональные компьютеры и дисплейные станции с возможностью сохранения ввода. Заполните часть 2 (Физическая защита рабочих станций и принтеров) формы Планирование физической защиты.

От чего следует защищать рабочие станции

Общедоступные рабочие станции

Если у посторонних есть свободный доступ к рабочим станциям, то они в принципе могут получить доступ и к конфиденциальной информации. Например, если пользователь системы отойдет от рабочего места, не выходя из системы, то его рабочей станцией может воспользоваться другой человек.

Физически скрытые рабочие станции

Рабочая станция, расположенная в скрытом, малопосещаемом месте, позволяет злоумышленнику потратить на взлом защиты системы несколько часов без риска быть обнаруженным.

Применение для входа в систему макрокоманды или программы PC

Многие дисплейные станции поддерживают запись и воспроизведение макрокоманд, позволяющих выполнять в системе большое количество операций нажатием одной клавиши. Если в качестве терминала применяется персональный компьютер, то вход в систему iSeries можно автоматизировать. Поскольку при каждом входе в систему пользователь выполняет одни и те же действия, он может сохранить свое имя и пароль в макрокоманде.

Рекомендации

При настройке физической защиты рабочих станций учтите следующие рекомендации:

- По возможности избегайте размещения рабочих станций в общедоступных или скрытых местах.
- Объясните пользователям важность выхода из системы в том случае, если они покидают свое рабочее место. Зафиксируйте это в требованиях для сотрудников.
- Объясните пользователям, что сохранение паролей в памяти рабочей станции или персонального компьютера нарушает защиту системы. Внесите этот пункт в требования для сотрудников.
- Настройте системные значения QINACTITV и QINACTMSGQ.
- Ограничьте возможности общедоступных рабочих станций, разрешив вход с этих станций только пользователям с ограниченными правами доступа.
- Ограничьте возможности физически скрытых рабочих станций, разрешив вход с этих станций только пользователей с ограниченными правами доступа. Для этого настройте системное значение QLMTSECOFR.

- Запретите пользователям одновременный вход в систему с нескольких дисплейных станций. Для этого настройте системное значение QLMTDEVSSN.

Более подробная информация о реализации этих рекомендаций приведена в разделе ″Выбор системных значений, управляющих входом в систему″ и ″Планирование защиты рабочих станций″.

Для заполнения формы Планирование физической защиты необходимо определить, какие рабочие станции могут применяться для нарушения защиты из-за их физического расположения. Вы можете ознакомиться с примером физической защиты рабочих станций в компании JKL Toys.

Следующий этап после завершения планирования защиты рабочих станций - это физическая защита принтеров и их вывода.

Физическая защита принтеров и вывода на принтер

Информацию, напечатанную на принтере, невозможно защитить с помощью настройки. Для предотвращения несанкционированного доступа к напечатанной конфиденциальной информации необходимо обеспечить защиту принтеров и выводимых на них данных. Внесите пункт о защите печатаемой информации в требования для сотрудников.

От чего следует защищать принтеры и выводимую на них информацию

Ниже перечислены наиболее часто встречающиеся ситуации, которые необходимо предусмотреть при планировании защиты. Для обеспечения наиболее полной защиты рассмотрите также другие возможные ситуации.

- Принтер, расположенный в общедоступном месте, позволяет посторонним лицам получить доступ к конфиденциальной информации.
- Оставленная на столе распечатка также может быть причиной утечки информации.
- К системе может быть подключен только один или два принтера. При печати на них такой информации, как ведомости по зарплате, конфиденциальность будет нарушена.

Рекомендации

Рекомендации по защите принтеров и выводимой на них информации:

- Объясните пользователям важность защиты конфиденциальной информации, выводимой на принтер. Включите соответствующие решения в требования для сотрудников.
- Не размещайте принтеры в общедоступных местах.
- Печатайте конфиденциальные данные в строго определенное время, когда рядом с принтером находится ответственный сотрудник.

Более подробно защита вывода на принтер обсуждается в разделе ″Планирование защиты принтеров и вывода на принтер″.

Вы можете ознакомиться с примером плана защиты принтеров компании JKL Toys. Следующий этап - планирование требований для сотрудников.

Пример: Форма План физической защиты компании JKL Toys—Рабочие станции: Ниже приведен пример второй части плана физической защиты, разработанного Шэрон Джонс для системы компании JKL Toys:

Таблица 5. Пример: Форма План физической защиты компании JKL Toys: рабочие станции и принтеры

План физической защиты			Часть 2 из 2
Физическая защита принтеров и рабочих станций			
Имя рабочей станции или принтера	Расположение или описание	Надежность защиты	Необходимые меры по защите

Таблица 5. Пример: Форма План физической защиты компании JKL Toys: рабочие станции и принтеры (продолжение)

DSP06	Склад	Станции общедоступны	Автоматический выход из системы. Ограничить функции, которые можно выполнять с этих рабочих станций.
DSP09	Отдел обслуживания клиентов	Станции общедоступны	Автоматический выход из системы. Ограничить функции, которые можно выполнять с этих рабочих станций.
RMT12	Удаленный торговый офис	Работа станции не контролируется	Не разрешать системному администратору входить в систему с этой станции.
PRT02	Бухгалтерия, рядом с системным блоком	Возможна печать конфиденциальной информации, такой как прейскуранты	Назначить сотрудника для контроля за выводом на принтер

После заполнения формы План физической защиты перейдите к разделу "Разработка стратегии защиты".

Планирование инструкций для сотрудников

Рекомендуется разработать письменные инструкции по защите и довести их до сведения всех сотрудников, работающих в компании, и принимаемых на работу.

Например, эти инструкции должны включать требование выходить из системы в том случае, если сотрудник покидает рабочее место, запрет на передачу личных паролей другим лицам, а также другие требования.

Отмечайте требования к защите по мере чтения этой книги.

Ниже приведен пример заметок, сделанных системным администратором компании JKL Toys Шэрон Джонс при планировании физической защиты:

```
Подчеркнуть важность выхода из системы для отделений работы с
клиентами и
удаленного офиса. Установить наблюдение за системным блоком.
```

После заполнения формы Планирование физической защиты перейдите к планированию защиты приложений.

Планирование защиты приложений

Перед тем, как приступить к планированию защиты приложений, вы должны ответить на следующие вопросы:

- Какая информация будет храниться в вашей системе?
- Кому необходим доступ к этой информации?
- Кому необходимы права на изменение информации, а кому - только на ее просмотр?

В первом разделе планирования защиты приложений вы должны определить, какая информация будет храниться в вашей системе. В последующих разделах вы сможете выбрать пользователей, которым необходим тот или иной тип доступа к информации. Информация о планировании защиты приложений не вводится в систему, но влияет на настройку защиты пользователей и ресурсов.

Что такое приложение?

На первом шаге планирования защиты приложений необходимо определить набор приложений, которые будут установлены в системе. Приложение - это группа функций, логически объединенных вместе. Например, в компании JKL Toys ввод заказов, отправка заказов и печать счетов - это функции одного приложения Заказы клиентов.

Обычно в системе iSeries работают приложения двух типов:

- **Деловые приложения:** приложения, купленные или разработанные для выполнения конкретных функций, таких как обработка заказов или управление запасами.
- **Специальные приложения:** приложения, применяемые компанией, но не связанные непосредственно с ее производственным процессом.

Необходимые формы

При планировании защиты приложений заполните следующие формы:

- Описание приложения
- Описание библиотеки
- Соглашения о присвоении имен

Для печати формы выберите фрейм, в котором она показана, и нажмите кнопку **Печать**.

Более подробно планирование защиты приложений и заполнение перечисленных форм обсуждается в следующих разделах:

- Создание описаний приложений
- Описание соглашений о присвоении имен
- Создание описаний библиотек
- Создание диаграммы приложений

Создание описаний приложений

На данном этапе планирования необходимо собрать информацию о приложениях, применяющихся в вашей компании. Внесите эту информацию в соответствующие поля формы Описание приложения согласно приведенным ниже инструкциям. Эта информация понадобится при планировании защиты групп пользователей и приложений:

Имя и сокращенное название приложения
: Присвойте приложению короткое имя и сокращенное название, которые вы сможете указывать в формах и названиях объектов, с которыми работает это приложение.

Описание
: Коротко опишите функции приложения.

Главное меню и библиотека
: Выберите главное меню приложения. Определите, в какой библиотеке оно находится. Обычно главное меню содержит ссылки на другие меню, обеспечивающие доступ к различным функциям приложения. Если указать главное меню приложения в профайле работающих с ним пользователей, то это меню будет показано сразу после входа пользователей в систему.

Начальная программа и библиотека
: Иногда приложения запускают начальную программу, задающую среду для работы приложения или проверяющую права доступа. Если у приложения есть такая программа, укажите ее в этом поле.

Библиотеки приложения
: С каждым приложением связана главная библиотека, в которой хранятся файлы этого приложения. Укажите в этом поле также все остальные библиотеки, к которым обращается приложение, включая библиотеки, в которых хранятся программы и библиотеки, которые относятся к другим приложениям. Например, приложение Заказы клиентов компании JKL Toys получает значения баланса и описания из библиотеки Запасы, принадлежащей приложению Управление запасами.

От связей между библиотеками и приложениями зависят права доступа пользователей к библиотекам.

Получение информации о приложениях

Если у вас нет всей необходимой информации о приложениях, установленных в системе, свяжитесь с разработчиками приложения.

Если вы не можете получить информацию от разработчиков приложения, соберите информацию самостоятельно:

- Узнайте название главного меню и библиотеки приложения у пользователей, работающих с ним, или просто понаблюдайте за их действиями после входа в систему.
- Если пользователи попадают в приложение сразу после входа в систему, проверьте параметр **Начальная программа** их пользовательских профайлов. В этом поле может быть указана начальная программа приложения. Для просмотра пользовательского профайла введите команду DSPUSRPRF.
- Просмотрите имена и описания всех библиотек системы. Для этого введите команду DSPOBJD *ALL *LIB.
- Просмотрите список активных заданий в то время, когда пользователи работают с приложениями. Подробную информацию об интерактивных заданиях можно получить с помощью команды Работа с активными заданиями на промежуточном уровне поддержки. Для получения информации об используемых библиотеках просмотрите сведения о блокировке объектов активными заданиями.
- Просмотрите пакетные задания приложений с помощью команды Работа с пользовательскими заданиями (WRKUSRJOB).

Для завершения сбора информации о приложениях выполните следующие действия:

- Заполните форму Описание приложения для каждого из установленных в системе приложений. В форме должен остаться незаполненным только раздел требований защиты. Этот раздел применяется при планировании защиты ресурсов (см. раздел ″Планирование защиты ресурсов″).
- Заполните форму Описание приложения для каждого из специальных приложений. Это необходимо для определения прав доступа к приложению.

Примечание: Заполнять формы Описание приложения для специальных приложений IBM, например, IBM Query для iSeries, необязательно. Доступ к библиотекам, с которыми работают эти приложения, не требует отдельного планирования. Однако, эти формы можно заполнить для полноты или в качестве тренировки.

Вы можете ознакомиться с примером формы Описание приложения компании JKL Toys. Следующий этап - описание соглашений о присвоении имен.

Пример: Форма Описание приложения компании JKL Toys: Шэрон Джонс перечислила в формах описания приложений все используемые в компании приложения, указав также их краткие названия. Кроме того, она описала работу пользователей с этими приложениями.

Заказы клиентов (CO)
Ввод, просмотр и обслуживание заказов. Печать счетов-фактур.

Управление запасами (IC)
Управление запасами произведенной продукции и сырья. Обработка всех перемещений сырья и продукции.

Контракты и цены (CP)
Управление особыми ценами и контрактами.

Дебиторская задолженность (AC)
Отслеживание текущего баланса. Печать ежемесячных отчетов.

В следующей таблице содержится описание приложения Заказы клиентов, составленное Шэрон Джонс. Она подготовила такие формы для всех приложений.

Таблица 6. Пример формы Описание приложения компании JKL Toys

Описание приложения	
Составлено: Шэрон Джонс	Дата: 9/3/99
Имя приложения: Заказы клиентов	Аббревиатура: CO
Краткое описание приложения:	Ввод заказов клиентов, отслеживание обработки заказов до момента поставки, поставка товаров, печать счетов-фактур и накладных.
Имя главного меню: COMAIN	Библиотека: COPGMLIB
Имя начальной программы: нд	Библиотека: нд
Перечислите библиотеки, используемые приложением для хранения файлов и программ: • CUSTLIB • ITEMLIB • CONTRACTS • COPGMLIB	
Определите требования по защите приложения, например, уровень конфиденциальности информации:	

Шэрон также подготовила формы Описание приложения для следующих приложений JKL Toys:

- Управление запасами
- Контракты и цены
- Дебиторская задолженность

Теперь вы можете перейти к описанию соглашений о присвоении имен объектам системы.

Описание соглашений о присвоении имен

Соглашения о присвоении имен необходимы для планирования и поддержания системы защиты, устранения неполадок, а также для планирования процедур резервного копирования и восстановления. Обычно при выборе имен объектов (библиотек, файлов и программ) в приложениях применяются довольно простые правила. Однако в приложениях разных разработчиков эти правила могут различаться.

Занесите соглашения о присвоении имен каждого приложения в форму Соглашения о присвоении имен. Перечислите в этой форме правила, по которым приложение выбирает имена для объектов. Занесите туда также другие соглашения о присвоении имен, например, относящиеся к программам и файлам меню. Если в системе установлены приложения, полученные из разных источников, их соглашения о присвоении имен могут отличаться. Опишите соглашения о присвоении имен для каждого из приложений. Для этого может потребоваться несколько форм.

Вы можете ознакомиться с примером формы Соглашения о присвоении имен компании JKL Toys. Следующий этап - создание описаний библиотек.

Пример: Форма Соглашения о присвоении имен в компании JKL Toys: В следующей таблице показаны соглашения о присвоении имен файлам и библиотекам. Вам также потребуется описать правила присвоения имен объектам других типов. Форма Соглашения о присвоении имен содержит записи для нескольких основных объектов. Возможно, вам потребуется описать и другие объекты.

Таблица 7. Пример формы Соглашение о присвоении имен в JKL Toys

Форма Соглашения о присвоении имен	
Составлено: Шэрон Джонс	Дата: 9/3/99

Таблица 7. Пример формы Соглашение о присвоении имен в JKL Toys (продолжение)

Тип объекта	Соглашение о присвоении имен
Библиотеки	Библиотеки, в которых хранятся файлы, имеют понятные имена, такие как CONTRACTS или ITEMLIB. Названия библиотек программ состоят из кратких имен программ и символов PGMLIB - например, ICPGMLIB.
Файлы	Большинство файлов имеет понятные имена, например CUSTMAST для основного файла записей о клиентах или ITEMMAST для основного файла записей о продуктах. Остальным файлам, используемым в приложениях, программисты присвоили имена, состоящие из краткого названия приложения, слова FILE и числа - например, ICFILE14.

После заполнения формы Соглашения о присвоении имен, вы можете перейти к описанию библиотек.

Создание описаний библиотек

После описания соглашений о присвоении имен создайте описания библиотек системы. Библиотеки предназначены для идентификации объектов и их упорядочения в системе. Размещение похожих файлов в одной библиотеке упрощает доступ пользователей к важным приложениям и файлам. Кроме того, библиотеки упрощают управление правами доступа. Создайте описание для библиотек всех приложений, установленных в вашей системе. Для этого могут потребоваться несколько форм Описание библиотеки

Примечание: На этом этапе заполните только поле Описание. Оставшуюся часть формы Описание библиотеки вы заполните при планировании защиты ресурсов. Информацию о правах доступа к библиотекам также нужно будет указать позже. Более подробная информации о заполнении оставшейся части формы приведена в разделе ″Планирование защиты библиотек приложений″.

Выполните следующие действия:

- Заполните части формы Соглашения о присвоении имен, относящиеся к библиотекам и файлам.
- Заполните поле Описание формы Описание библиотеки для всех библиотек каждого приложения.

Вы можете ознакомиться с примером формы Описание приложения для компании JKL Toys. Следующий этап - создание диаграммы приложений.

Пример: Форма Описание библиотеки компании JKL Toy: В приведенных ниже таблицах описаны две библиотеки, используемые приложением Заказы клиентов. Первая таблица описывает библиотеку, в которой хранятся файлы, а вторая - библиотеку, в которой хранятся программы.

Таблица 8. Пример формы Описание библиотеки компании JKL Toys: Библиотека файлов

Форма Описание библиотеки	
Составлено: Шэрон Джонс	Дата: 9/3/99
Имя библиотеки: CUSTLIB	Описание: Библиотека с информацией о клиентах
Кратко опишите назначение библиотеки:	В библиотеке хранятся все записи о клиентах, включая файлы заказов и счетов.

Таблица 9. Пример формы Описание библиотеки компании JKL Toys: Библиотека программ

Форма Описание библиотеки	
Составлено: Шэрон Джонс	Дата: 9/3/99
Имя библиотеки: COPGMLIB	Описание: Библиотека программы клиентских заказов
Кратко опишите назначение библиотеки:	В библиотеке хранятся все программы, используемые приложением Заказы клиентов.

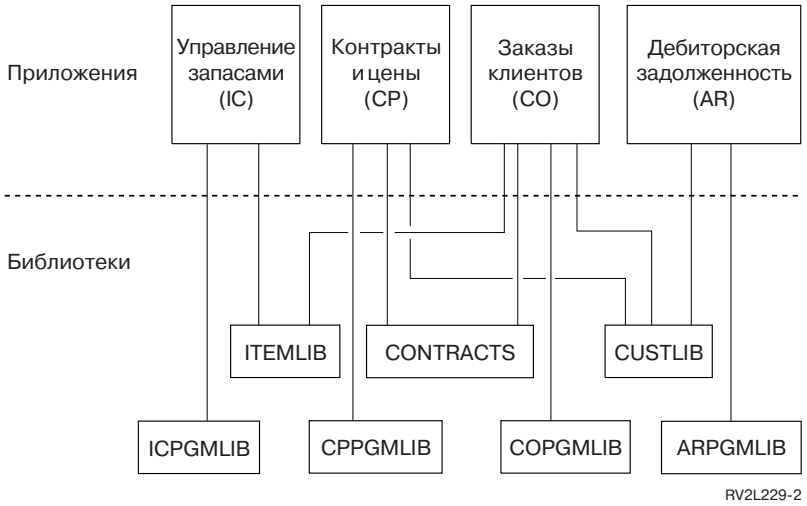
После того, как вы описали библиотеки, вы должны составить диаграмму приложений в системе.

Создание диаграммы приложений

При заполнении форм Описание приложения и Описание библиотеки вам может потребоваться составить диаграмму с указанием взаимосвязи между приложениями и библиотеками. Кроме того, эта диаграмма поможет составить план защиты пользователей и ресурсов.

На следующем рисунке показана диаграмма, составленная Шэрон Джонс для системы AS/400 компании JKL Toys.

Диаграмма приложений и библиотек для компании JKL Toys



Информация о связи приложений и библиотек необходима для принятия многих решений, имеющих отношение к защите. Рассматривайте создание диаграммы как дополнительную возможность побольше узнать о своей системе.

Перед созданием диаграммы выполните следующие действия:
- Заполните форму Описание приложения для каждого делового приложения, установленного в системе.
- Заполните форму Описание приложения для каждого установленного в системе специального приложения (этот шаг можно пропустить).
- Заполните разделы Библиотеки и файлы формы Соглашения о присвоении имен.
- Подготовьте форму Описание библиотеки для каждой библиотеки системы.
- Нарисуйте диаграмму, на которой показана связь между приложениями и библиотеками в вашей системе.

Следующий этап - планирование общей стратегии защиты.

Планирование общей стратегии защиты

После планирования защиты приложений вы можете перейти к планированию общей стратегии защиты. Для этого сначала необходимо определить общий подход к организации защиты вашей системы. Кроме того, необходимо учесть как текущие, так и будущие требования к защите.

Общая стратегия защиты поможет вам определить цели защиты и завершить планирование. Кроме того, от нее зависит настройка основных системных значений, влияющих на всех пользователей системы.

Необходимые формы

При завершении планирования защиты приложений вам потребуется форма Выбор системных значений.

Для принятия решений о системных значениях потребуются формы Планирование физической защиты и Описание приложения.

Просмотрите следующие разделы:

- Определение стратегии защиты
- Выбор уровня защиты
- Выбор системных значений, связанных с входом в систему
- Выбор системных значений, связанных с паролями
- Настройка системных значений

Определение стратегии защиты

Перед началом планирования необходимо выработать общую стратегию вашей компании в сфере защиты информации. Эта стратегия должна быть сформулирована руководством компании. Все решения по защите должны приниматься в соответствии с выбранной стратегией. Стратегия должна определять общий подход к вопросам защиты и включать конкретный перечень информационных ресурсов, требующих защиты.

Любая система должна быть защищена. Вы можете выбрать один из следующих подходов к защите:

- **Строгая стратегия:** минимизация прав доступа. В случае применения строгой стратегии защиты пользователям предоставляются только те права доступа, которые необходимы им для работы. Доступ ко всей остальной информации запрещается. Многие аудиторы рекомендуют применять именно такую стратегию защиты.
- **Промежуточная стратегия:** доступ пользователей к объектам зависит от предоставленных им прав.
- **Упрощенная стратегия:** пользователям разрешен доступ к большинству объектов системы. Доступ ограничивается только к особо важным или конфиденциальным ресурсам. Обычно эта стратегия применяется небольшими компаниями.

Определение общего подхода к защите поможет вам при принятии конкретных решений. Защита системы должна соответствовать общему подходу к защите информации, принятому в вашей компании. Если вы не знаете, какую стратегию лучше выбрать, то воспользуйтесь следующими рекомендациями:

- Определите права доступа, необходимые каждому пользователю. Для этого просмотрите формы Описание приложения.
- Проверьте технологии, которые будут применяться в вашей компании. Например, если ваша система или сеть будет подключена к Internet, рекомендуется усилить ее защиту.
- Обсудите стратегию защиты с другими сотрудниками, например с аудиторами защиты.

Помните, что вы всегда можете изменить стратегию защиты. Большинство компаний по мере роста делают защиту более строгой. Эта информация поможет вам настроить защиту таким образом, чтобы потом ее можно было усилить, не затрачивая на этом много сил и времени, и не проверяя повторно все приложения.

Что следует защищать

Кроме выбора общего подхода к защите необходимо определить, какие именно объекты нуждаются в защите. При выборе защищаемой информации особое внимание следует обратить на сведения, обладающие следующими характеристиками:

- **Конфиденциальность:** информация недоступна большинству персонала компании. Пример: ведомости по зарплате.
- **Уникальность:** информация, которая дает вам преимущества перед конкурентами.
- **Важность:** информация необходима для работы компании. Пример: сведения о заказчиках.

Шэрон Джонс, системный администратор и Джон Смит, президент компании, разработали стратегию защиты компании JKL Toys. В процессе работы Джон Смит записал некоторые свои замечания. Просмотрите письмо о стратегии защиты, разосланное сотрудникам компании JKL Toys после завершения планирования и настройки защиты. Замечания Джона Смита приведены ниже.

Таблица 10. Пример стратегии защиты для компании JKL Toys

Общий подход

Упрощенная стратегия: У большинства пользователей есть доступ к большей части информации.

Важная информация

- Контракты и особые цены
- Ведомости по зарплате
- Сведения о клиентах и запасах доступны только сотрудникам компании.

Общие правила

- Для каждого пользователя системы будет создан пользовательский профайл. Пользователи не должны совместно использовать профайлы и передавать друг другу пароли.
- Пароли пользователей должны меняться каждые 60 дней.

Следующий этап - выбор уровня защиты.

Выбор уровня защиты

Системное значение QSECURITY - это один из основных параметров защиты системы AS/400. Лучше понять различие между уровнями защиты вам поможет аналогия со зданием.

Уровень 20: Защита с помощью паролей

Значение 20 обеспечивает минимальную защиту. Все пытающиеся войти в здание должны назвать свое имя и секретный пароль. Войти в здание смогут только люди, знающие и имя, и пароль. Однако все, кто попал внутрь, могут свободно перемещаться по зданию и делать все, что хотят.

Для взлома защиты достаточно узнать пароль любого пользователя и войти в здание.

Уровень 30: Защита с помощью паролей и защита ресурсов

На уровне 30 к системе защиты уровня 20 добавляется управление доступом к отдельным частям здания. Вы можете определить, какие люди имеют доступ к определенной части здания, и какие операции они могут выполнять, находясь в этой части. Некоторые части здания могут быть общедоступными, а вход в некоторые части может быть ограничен.

Кроме того, некоторые люди смогут сами выполнять в защищенных частях здания определенные действия, а некоторые должны будут делать запросы через уполномоченных представителей (программы). Чужого пароля по прежнему может оказаться достаточно для прохода в здание, включая его защищенные части.

Уровень 40: Защита целостности

На уровне 40 к средствам защиты уровня 30 добавляется дополнительная проверка пользователей. Охранники внутри здания проверяют пароли и записывают сведения обо всех входящих пользователях.

Уровень 50: Расширенная защита целостности

На уровне 50 при проверке всех сотрудников, находящихся в защищенных частях здания, охранники руководствуются более жестким набором правил.

Рекомендации

Системы iSeries поставляются с уровнем защиты 40. Этот уровень защиты является оптимальным в большинстве случаев для любой стратегии защиты - от строгой до упрощенной. Для реализации упрощенной стратегии защиты достаточно настроить общий доступ к большинству ресурсов системы. Выбор с самого начала уровня защиты 40 упростит усиление защиты в будущем.

При покупке приложений убедитесь в том, что они тестировались на совместимость с уровнем защиты 40. Приложения могут пытаться выполнять операции, которые при уровне защиты 40 приведут к

возникновению ошибок. Если некоторые приложения, установленные в вашей системе, не проверялись с уровнем защиты 40, установите уровень защиты 30. С помощью журнала контроля проверьте, не возникают ли при работе приложений ошибки, связанные с неправильными правами доступа. Если таких ошибок нет, увеличьте уровень защиты до 40 или 50.

Уровень защиты предназначен для предотвращения сравнительно редких событий, которые в большинстве систем никогда не происходят. При этом система дополнительно проверяет все работающие программы. Это может снизить общую производительность системы.

Внесите выбранный уровень защиты в форму Выбор системных значений. Следующий этап - выбор системных значений, управляющих входом в систему.

Выбор системных значений, связанных с входом в систему

После выбора уровня защиты можно перейти к настройке системных значений, управляющих входом пользователя в систему. Записывайте выбранные системные значения в форму Выбор системных значений.

Системные значения, обсуждаемые в этом разделе, перечислены в следующей таблице:

Таблица 11. Системные значения iSeries и их описания

Системное значение	**Описание**
QMAXSIGN	Максимальное число последовательных неудачных попыток входа в систему.
QMAXSGNACN	Действие, выполняемое системой при превышении максимального числа попыток входа в систему.
QLMTDEVSSN	Запрещение пользователям входить в систему с нескольких рабочих станций одновременно.
QINACTITV	Максимальное время неактивности задания.
QINACTMSGQ	Действие, выполняемое системой для задания, которое было неактивным на протяжении времени, указанного в системном значении QINACTITV.
QDSCJOBITV	Указывает, нужно ли завершать временно отсоединенные задания.
QLMTSECOFR	Разрешает администратору защиты вход в систему только с указанных устройств

Ограничение числа попыток входа в систему (QMAXSIGN и QMAXSGNACN): Максимальное число попыток входа в систему и действие, выполняемое при превышении этого ограничения, задаются двумя системными значениями.

Значение QMAXSIGN (Максимальное число попыток входа в систему) задает максимальное допустимое число неудачных последовательных попыток входа в систему. Неудачной попыткой входа в систему называется ситуация, когда пользователь вводит неправильный пароль или пытается войти в систему с рабочей станции, с которой ему это запрещено.

Значение QMAXSGNACN (Действие при превышении максимального числа попыток) указывает, что система должна сделать в том случае, если пользователь совершит слишком много неудачных попыток входа в систему подряд. Возможны следующие значения:

1 Запретить вход в систему с данного устройства. Эта операция называется отключением устройства. Никто не сможет войти в систему с указанного устройства до тех пор, пока оно не будет включено с помощью команды WRKCFGSTS. В целом можно сказать, что данная опция обеспечивает недостаточную защиту, особенно если злоумышленник пытается войти в вашу систему с персонального компьютера или из удаленной системы.

Любой пользователь с правами доступа *USE к устройству может снова включить его.

2 Запретить вход в систему для указанного пользовательского профайла. Эта операция называется отключением профайла. Данный пользователь не сможет войти в систему до тех пор, пока профайл не будет включен с помощью команды CHGUSRPRF (Изменить пользовательский профайл).

Изменять состояние профайлов могут только администраторы системы, у которых есть права доступа на использование данного профайла.

3 Отключить устройство и профайл.

Степень защиты и рекомендации

Некоторые злоумышленники пытаются войти в чужие системы путем подбора паролей. Если вы ограничите максимальное число неудачных попыток входа в систему, вы существенно снизите вероятность такого проникновения в систему.

Системное значение QMAXSIGN задает максимальное разрешенное число попыток входа в систему. Это значение должно быть достаточно большим на случай непреднамеренных ошибок при вводе пароля. С другой стороны, чем меньше это значение, тем меньше шансов на вход в систему будет у злоумышленников, пытающихся угадать пароль. Рекомендуем вам установить это значение в диапазоне от 3 до 5.

Системному значению QMAXSGNACN рекомендуется присваивать значение 3, хотя это и может создать определенные неудобства для пользователей системы. Однако в противном случае у злоумышленника, работающего на удаленной рабочей станции, будет возможность попробовать войти в систему от имени различных пользователей. Защиты, предусмотренной опцией 2 (отключение профайла), достаточно только в том случае, если к вашей системе не подключены удаленные рабочие станции.

Просмотрите форму физической защиты. Если в системе применяются удаленные рабочие станции или если какие-либо пользователи подключаются к системе по телефонным линиям или соединениям VPN, то опции 2 будет явно недостаточно. Обязательно занесите выбранные вами значения QMAXSIGN и QMAXSGNACN во вторую часть формы выбора системных значений.

Рекомендуем вам просмотреть пример, иллюстрирующий применение этих системных значений. Теперь вы можете задать системные значения, ограничивающие одновременное число сеансов для пользователей.

Пример: ограничение числа попыток входа в систему: Шэрон Джонс разрешила выполнять не более 3 попыток входа в систему (системное значение QMAXSIGN равно 3); в случае превышения этого ограничения пользовательский профайл и устройство будут отключены (системное значение QMAXSGNACN равно 3). Предположим, что возникла следующая ситуация:

1. Пользователь Роджер дважды неправильно ввел пароль.
2. После второй попытки он получил сообщение о том, что если он еще раз неверно введет пароль, его профайл будет отключен.
3. Не придав этому сообщению особого значения, Роджер и в третий раз неправильно ввел пароль.
4. В результате профайл Роджера был отключен, а на рабочей станции пропало меню входа в систему. Если Роджер попытается войти в систему с другой рабочей станции, будет показано сообщение об ошибке.
5. Теперь для входа к систему ему нужно сначала обратиться к Шэрон. Помимо профайла, Шэрон и оператору нужно будет включить рабочую станцию Роджера. Если Роджер забыл свой пароль, Шэрон может выдать ему временный пароль, который он должен будет изменить сразу после входа в систему.

Теперь вы можете перейти к системному значению, ограничивающему возможности системного администратора.

Разрешение входа в систему только с одной рабочей станции: Системное значение QLMTDEVSSN (Ограничить сеансы одним устройством) указывает, может ли пользователь войти в систему одновременно с нескольких рабочих станций. Возможны следующие значения:

0 Под управлением одного пользовательского профайла в системе может работать неограниченное число пользователей.

1 Под управлением конкретного пользовательского профайла в каждый момент времени может работать только одно устройство. Однако у пользователя может быть запущено несколько сеансов работы с одним устройством.

Степень защиты и рекомендации

Запрет на одновременную работу пользователя на нескольких рабочих станциях - это хорошая практика защиты. Не сделав этого, вы откроете следующие возможности проникновения в систему:

- Если пользователям будет запрещено работать на нескольких рабочих станциях одновременно, у них не будет причин сообщать друг другу свои идентификаторы и пароли. Как только пользователи начинают сообщать друг другу свою учетную информацию, вы теряете всякий контроль над их работой. Вы никогда не сможете сказать, кто на самом деле работает в системе.
- Пользователей следует обязать выходить из системы перед переходом на другую рабочую станцию. В противном случае они начнут оставлять рабочие станции без присмотра, не выходя из системы, а это представляет собой серьезную опасность.

Рекомендуем вам присвоить QLMTDEVSSN значение 1 (ограничить сеансы одним устройством). Предоставьте всем пользователям собственные идентификаторы, пароли и права доступа и запретите им работать на нескольких станциях одновременно. Обязательно запишите значение QLMTDEVSSN во вторую часть формы выбора системных значений.

Теперь можно перейти к настройке системных значений для простаивающих заданий.

Настройка системных значений для простаивающих заданий: Для управления обработкой простаивающих заданий (такие задания возникают, например, когда пользователь забывает выйти из системы) применяются три системных значения.

Тайм-аут простаивающих заданий (QINACTITV)
Системное значение QINACTITV определяет, будет ли система предпринимать какие-либо действия по отношению к дисплеям, с которых был выполнен вход в систему, но которые простаивают в течение заданного промежутка времени.

Примечание: **Простаивающим** называется задание, в котором пользователь не нажимал клавишу Enter и другие функциональные клавиши в течение заданного времени.

Очередь сообщений простаивающих заданий (QINACTMSGQ)
Системное значение QINACTMSGQ указывает, какие действия система предпринимает по отношению к заданиям, простаивающим свыше ограничения, указанного с помощью системного значения QINACTITV. Если вы укажете значение ENDJOB, система будет пытаться завершить задания, простаивающие в течение времени, превышающего указанное в QINACTITV. Если вы укажете значение DSCJOB, система будет прерывать соединения простаивающих заданий. Если вы укажете имя очереди сообщений, то по приближении тайм-аута в эту очередь будет направлено предупреждающее сообщение.

Если система **отсоединяет** задание, то задание временно приостанавливается. На рабочей станции появляется меню входа в систему. Выполнение отсоединенного задания возобновляется при следующем входе пользователя в систему с той же рабочей станции.

Тайм-аут отсоединенных заданий (QDSCJOBITV)
Системное значение QDSCJOBITV определяет, завершается ли работа временно отсоединенных заданий, и если завершается, то когда. Задания могут быть отсоединены как автоматически (на основании значений QINACTITV и QINACTMSGQ), так и вручную (с помощью меню операционной поддержки или команды DSCJOB).

Степень защиты и рекомендации

Если, уходя с работы, Шэрон забудет выйти из системы, то любой другой пользователь сможет подойти к ее рабочей станции и выполнить любые действия, разрешенные Шэрон.

Управление простаивающими дисплеями целесообразно в следующих случаях:

- В вашей системе хранится конфиденциальная информация, требующая надежной защиты.
- Рабочие станции расположены таким образом, что ими могут воспользоваться посторонние люди.

Зачастую по долгу службы сотрудникам приходится отходить от рабочих станций. Разумное применение данных системных значений позволит снизить риск нарушения защиты даже с учетом того, что сотрудники не всегда находятся на своих рабочих местах.

Фирма IBM рекомендует выбрать такие значения QINACTITV, QINACTMSGQ и QDSCJOBITV, чтобы ваши сотрудники могли безболезненно отвлекаться от работы, но при этом был минимален риск того, что система станет доступна посторонним лицам.

Тайм-аут простаивающих заданий (QINACTITV): это значение должно быть небольшим, чтобы рабочие станции можно было безбоязненно оставлять без присмотра, но в то же время достаточным для того, чтобы пользователям не приходилось все время следить за своим сеансом. Рекомендуемое значение - 30 минут. Если задание будет простаивать более 30 минут, система будет выполнять действие, указанное в системном значении QINACTMSGQ,

Очередь сообщений простаивающих заданий (QINACTMSGQ): рекомендуем указать значение *DSCJOB. В этом случае система будет отсоединять задания, время простоя которых превысит ограничение, заданное в системном значении QINACTTMR. Помимо отсоединения задания, рабочая станция будет отключена от системы. При следующем входе пользователя в систему с той же рабочей станции выполнение задания будет возобновлено.

Такой режим более удобен для пользователей, потому что их задания в случае простоя будут не завершаться, а только приостанавливаться. При этом отсоединение заданий обеспечивает такую же защиту, что и их завершение.

Примечание: Некоторые задания отсоединить невозможно. Такие задания при возникновении тайм-аута завершаются. Это может привести к потере информации. Поэтому в некоторых случаях разумно указать в системном значении QINACTMSGQ опцию отправки предупреждающих сообщений в очередь системного оператора.

Тайм-аут отсоединенных заданий (QDSCJOBITV): пользователям следует временно выходить из системы, когда им нужно ненадолго отойти от рабочей станции, и завершать работу и выходить из системы в случаях, когда они прерывают работу на длительное время.

Системное значение QDSCJOBITV указывает, через какое время отсоединенное задание должно автоматически завершаться. Это системное значение применяется в тех случаях, когда вы хотите прервать выполнение пользовательских заданий (например, для выполнения автоматической очистки по ночам). Это значение должно быть достаточно большим, чтобы пользователи могли успеть вернуться на работу после перерыва без завершения их заданий, но и достаточно малым для того, чтобы все задания завершались к началу периодически выполняемой очистки. Рекомендуем вам установить этот интервал равным 300 минутам.

Примечание: Во избежание одновременного изменения одной и той же информации несколькими пользователями система **блокирует** записи перед обновлением. При отсоединении задания все блокировки ресурсов остаются в силе. При неудачном сочетании характеристик приложений и числа пользователей это может привести к снижению производительности системы. Информацию о том, насколько блокировка может повлиять на производительность системы, можно получить у ваших программистов или поставщиков программного обеспечения.

Рекомендуем вам ознакомиться с примером применения данных системных значений.

После того как вы подберете нужные значения и запишете их в форму выбора системных значений, можно переходить к ограничению возможностей системного администратора.

Пример: Работа с простаивающими заданиями с использованием системных значений QINACTITV, QINACTMSGQ и QDSCJOBITV: Предположим, что в системе установлен тайм-аут простоя заданий (QINACTITV) 30 минут. Неактивные задания отключаются (QINACTMSGQ имеет значение DSCJOB). Тайм-аут отключенных заданий (QDSCJOBITV) составляет 300 минут (5 часов). Например, если Шэрон забудет выйти из системы в 9:30, система отключит ее задание в 10:00 и завершит его в 15:00.

Запишите значения QINACTITV, QINACTMSGQ и QDSCJOBITV во второй части формы Настройка системных значений.

После того, как вы установили системные значения для бездействующих заданий, вы можете перейти к принятию решений об ограничении списка рабочих станций, с которых системный администратор может войти в систему.

Ограничение возможностей системного администратора: Вы можете задать список рабочих станций, с которых в систему могут входить пользователи с правами доступа, допускающими изменение параметров защиты. В этом случае пользователи с такими правами доступа не смогут без вашего ведома войти в систему с произвольных удаленных систем. Для задания таких ограничений применяется системное значение QLMTSECOFR (Ограничить возможности системного администратора). Если значение QLMTSECOFR равно 1, то пользователи с правами доступа *ALLOBJ и *SERVICE смогут входить в систему только с системной консоли и указанных вами рабочих станций.

Параметр QLMTSECOFR действует по отношению к пользователю QSECOFR и пользователям с правами доступа *ALLOBJ и *SERVICE. Для того чтобы предоставить этим пользователям доступа к другим устройствам, можно воспользоваться командой GRTOBJAUT (Предоставить права доступа к объектам).

Примечание: Системное значение QLMTSECOFR применяется только в случае, если для системы установлен уровень защиты не ниже 30.

Степень защиты и рекомендации

Рекомендуем присвоить QLMTSECOFR значение 1. Даже если кто-нибудь узнает пароль системного администратора, для входа в систему ему потребуется получить доступ к системной консоли.

После выбора значения QLMTSECOFR запишите его во второй части формы выбора системных значений и перейдите к выбору системных значений, связанных с паролями.

Выбор системных значений, связанных с паролями

Пароли пользователей должны выбираться ими самими, а не назначаться системным администратором. При создании паролей пользователи не должны записывать их. Записанные пароли часто хранятся в очевидных и доступных местах, представляя опасность с точки зрения защиты.

Совет по созданию паролей

Пользователи не всегда могут придумать хороший пароль. Предложите им следующий способ: придумайте фразу, которую легко запомнить, но трудно угадать, и возьмите первую букву от каждого слова. Например, после отпуска вы можете выбрать фразу ″May 1st fishing was poor″ (1 мая рыбалка была плохая), которой будет соответствовать пароль `M1FWP`.

Допустимость пароля зависит от системных значений. Вы можете задать минимальную частоту смены пароля. Кроме того, можно задать множество правил, предотвращающих задание очевидных паролей. Большая часть этих параметров применяется только в больших организациях. Однако есть ряд особенностей, о которых следует помнить всем.

Пользователь может изменить свой пароль с помощью опции меню ASSIST или команды Изменить пароль (CHGPWD). При этом система проверяет новый пароль на соответствие заданным системным значениям. При изменении пароля командой CHGUSRPRF он не проверяется на соответствие системным значениям.

Примечание: Если задано любое из системных значений, связанных с паролями, система не допустит, чтобы новый пароль совпадал со старым. Эта проверка не выполняется при изменении пароля командой CHGUSRPRF.

Системные значения, влияющие на выбор паролей, перечислены в следующей таблице:

Таблица 12. Системные значения iSeries, связанные с паролями

Системное значение	**Описание**
QPWDEXPITV	Пользователи должны менять свои пароли через указанное время.
QPWDMAXLEN	Максимальная длина пароля.
QPWDMINLEN	Минимальная длина пароля.
QPWDRQDDIF	Запрещает пользователям попеременно использовать два или несколько фиксированных паролей.

Дополнительная информация о системных значениях, связанных с выбором паролей, приведена в следующих разделах:

- Определение срока действия паролей
- Определение длины паролей
- Запрещение повторяющихся паролей

Введите в командной строке AS/400 команду `WRKSYSVAL *SEC` и просмотрите системные значения, имена которых начинаются с символов QPWD.

Настройка срока действия паролей: С помощью системного значения QPWDEXPITV можно задать максимальный срок действия паролей.

Когда срок действия пароля подойдет к концу, система предупредит пользователя о необходимости сменить пароль. По истечении срока действия пароля система потребует изменить пароль при очередном входе в систему.

Рекомендации

Пользователи должны регулярно изменять свои пароли. Это значительно снижает вероятность того, что кто-либо будет работать под управлением чужого профайла. Кроме того, если злоумышленник все-таки узнает чей-либо пароль, он будет действовать только в течение ограниченного времени. Однако срок действия паролей не должен быть очень коротким - это будет раздражать пользователей. Оптимальный срок составляет от 45 до 60 дней.

Запишите значение QPWDEXPITV во второй части формы выбора системных значений и перейдите к выбору длины паролей.

Выбор оптимальной длины паролей: Некоторые пользователи не любят работать с клавиатурой. Если бы они могли, они бы сократили свой пароль до одной буквы. К сожалению, такие пароли - это самый лакомый кусочек для злоумышленников, пытающихся подобрать пароли. С помощью системного значения QPWDMINLEN вы можете ограничить минимальную длину паролей, используемых в вашей системе.

Если ваша система подключена к другим, то для доступа к разным системам пользователи могут использовать одни и те же пароли. Некоторые протоколы связи могут работать только с паролями длиной не более 8 символов. С помощью системного значения QPWDMAXLEN можно ограничить максимальную допустимую длину паролей.

Рекомендации

Рекомендуем вам установить минимальную допустимую длину пароля равной 6 символам. В этом случае пользователям придется проявить изобретательность при выборе паролей. Если ваша система подключена к другим системам, рекомендуем также ограничить максимальную длину паролей 8 символами.

После выбора значений QPWDMINLEN и QPWDMAXLEN запишите их во второй части формы выбора системных значений и перейдите к ограничению на использование одинаковых паролей.

Ограничение на использование одинаковых паролей: Команда CHGPWD (Изменить пароль) устроена таким образом, что новый пароль всегда должен отличаться от прежнего. Однако пользователи могут ограничиться всего двумя паролями, используя их попеременно. Для предотвращения такой ситуации служит системное значение QPWDRQDDIF. В следующей таблице перечислены возможные значения QPWDRQDDIF:

Таблица 13. Системное значение QPDRQDDIF

Значение	Число предыдущих паролей, которые должны отличаться от нового
0	Все пароли должны быть разными.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Рекомендации

Максимальный срок действия паролей и ограничение на повторное применение паролей должны быть такими, чтобы в течение года использовались только различные пароли. Таким образом, если срок действия паролей составляет 60 дней, значение QPWDRQDDIF должно быть равно 7.

Запишите значение QPWDRQDDIF во второй части формы выбора системных значений и перейдите к настройке системных значений.

Настройка системы с помощью системных значений

Системные значения и сетевые атрибуты iSeries представляют собой основные инструменты управления работой системы. Системные и прикладные программисты активно пользуются большинством из них. Перед началом эксплуатации системы администратор должен настроить основные системные значения и сетевые атрибуты.

Присвоение имени системе

Имя системы задается сетевым атрибутом SYSNAME. Оно показано в верхнем правом углу меню входа в систему и во всех отчетах системы. Кроме того, имя системы используется при обмене данными с другими системами и персональными компьютерами с помощью iSeries Access для Windows.

Если ваша система будет обмениваться данными с другими системами и персональными компьютерами, необходимо, чтобы ее имя отличалось от имен других систем в сети. Компьютеры обмениваются своими

именами всякий раз при передаче данных. Настоятельно не рекомендуется изменять имя системы после того, как оно будет назначено впервые, так как это может потребовать дополнительной настройки других систем.

Рекомендации

Имя системы должно быть осмысленным. Даже если сейчас ваша система не будет подключена к другим, это вполне может произойти в будущем. Если ваша система будет подключена к сети, то, скорее всего, имя для нее будет предложено администратором сети.

Например, Шэрон Джонс из компании JKL Toys решила присвоить системе AS/400 имя JKLTOY.

Просмотр даты и времени

Система AS/400 поддерживает различные форматы представления даты. Помимо порядка следования компонентов даты, вы также можете задать символ разделителя.

Формат даты задается системным значением QDATFMT. В следующей таблице приведены все возможные способы представления даты 16 июня 2000 года:

Таблица 14. QDATFMT (Формат даты)

Выбранный вариант	Описание	Пример
YMD	Год, месяц, день	00/06/16
MDY	Месяц, день, год	06/16/00
DMY	День, месяц, год	16/06/00
JUL	Юлианский формат	00/168

Примечание: В этих примерах в качестве разделителя применяется косая черта (/).

Символ разделителя задается с помощью системного значения QDATSEP. Возможные варианты перечислены в следующем списке:

Таблица 15. QDATSEP (Разделитель даты)

Символ разделителя	Значение QDATSEP	Пример
/ (косая черта)	1	16/06/00
- (дефис)	2	16-06-00
. (точка)	3	16.06.00
, (запятая)	4	16,06,00
(пробел)	5	16 06 00

Примечание: В данных примерах применяется формат даты DMY.

Системное значение QTIMSEP задает разделитель времени (символ между значениями часов, минут и секунд). В следующей таблице перечислены возможные разделители времени:

Таблица 16. QTIMSEP (Разделитель времени)

Символ разделителя	QTIMSEP	Пример
: (двоеточие)	1	10:30:00
. (точка)	2	10.30.00
, (запятая)	3	10,30,00
(пробел)	4	10 30 00

Присвоение имен устройствам системы

Система AS/400 автоматически настраивает подключаемые к ней новые дисплейные станции и принтеры. Каждому новому устройству присваивается уникальное имя. Способ выбора имен зависит от системного значения QDEVNAMING. В следующей таблице указано, какие имена будут присвоены третьей дисплейной станции и второму принтеру, подключенным к системе, при различных значениях QDEVNAMING:

Таблица 17. Имена устройств системы

Выбранный вариант	Формат имен	Имя дисплейной станции	Имя принтера
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	Адрес устройства	DSP010003	PRT010002

Примечание: В данном примере предполагается, что дисплейная станция и принтер подключены к первому кабелю.

Рекомендации

Если вы не работаете с программами, в которых требуется применять соглашения о присвоении имен S/36, то рекомендуется использовать соглашения о присвоении имен iSeries. В системе iSeries дисплейным станциям и принтерам присваиваются более осмысленные и интуитивно понятные имена. Имена дисплейных станций и принтеров можно увидеть в нескольких меню операционной поддержки. Кроме этого, имена принтеров применяются в средствах управления выводом.

После того, как система создаст новое устройство, вы можете задать его текстовое описание с помощью команды CHGDEVDSP (Изменить устройство - дисплей) или CHGDEVPRT (Изменить устройство - принтер). Рекомендуется указывать в описаниях физические адреса и расположение устройств, например, *Офис Джона Смита, линия 1, адрес 6*.

Выбор системного принтера

Системное значение QPRTDEV задает системный принтер по умолчанию. Помимо этого значения, при выборе принтера для печати конкретного документа учитываются параметры пользовательского профайла и описания задания, выполняющего печать. Системный принтер по умолчанию применяется в случаях, когда в пользовательском профайле и описании задания не указано иное.

Рекомендации

Системным принтером по умолчанию должен быть самый быстрый из подключенных к системе принтеров. Системный принтер следует применять для печати больших отчетов и служебного вывода системы.

Примечание: Имена принтеров назначаются после установки и настройки системы. Рекомендуем вам сразу записать расположение системного принтера. Имя для него можно будет выбрать позже.

Просмотр напечатанных объектов вывода

Пользователи системы всегда могут определить, на каких принтерах печатаются их буферные файлы. В меню Работа с выводом на принтер можно просмотреть список буферных файлов, как печатающихся, так и находящихся в очереди. Кроме того, вы можете предоставить пользователям доступ к списку напечатанных файлов. В этом списке указано время печати и принтер для каждого напечатанного буферного файла. Данный список может пригодиться для поиска напечатанных отчетов.

Возможность просмотра информации о напечатанных буферных файлах обеспечивается с помощью средств учета заданий. Для управления этими средствами применяется системное значение QACGLVL. Если вы хотите, чтобы в системе сохранялась информация о напечатанных буферных файлах, присвойте QACGLVL значение *PRINT.

Рекомендации

Информация о напечатанных файлах хранится в системе и поэтому занимает часть системных ресурсов. Эта информация бывает действительно нужна только в том случае, если пользователи системы будут печатать очень много данных. Скорее всего, это не так, и поэтому в большинстве ситуаций системному значению QACGLVL следует присвоить значение *NONE и указать НЕТ в форме выбора системных значений.

- Обязательно разработайте для вашей организации стратегию защиты. Для этого можно воспользоваться примером стратегии защиты, разработанной Шэрон Джонс и Джоном Смитом для фирмы JKL Toys.
- Запишите все системные значения в форму выбора системных значений.
- Создайте памятку с правилами защиты.

После заполнения формы выбора системных значений и разработки стратегии защиты можно перейти к планированию пользователей и групп.

Пример: Стратегия защиты компании JKL Toys: Ниже приведено письмо о стратегии защиты компании JKL Toys, переданное сотрудникам компании ее президентом Джоном Смитом. При составлении письма использовались материалы, собранные президентом и Шэрон Джонс.

Таблица 18. Пример: Информация о стратегии защиты компании JKL Toys

От кого: Джон Смит, президент

Таблица 18. Пример: Информация о стратегии защиты компании JKL Toys (продолжение)

JKL Toys

Кому: Всем сотрудникам компании JKL Toys

Тема: Защита новой системы

Вы все присутствовали на собрании, посвященном новой системе. Те из вас, кто будет использовать эту систему, уже приступили к обучению и начнут обработку заказов на следующей неделе. Мы ожидаем, что система быстро станет важным элементом нашего бизнеса.

Я хочу осветить наши планы по защите системы и отметить их важность. Стратегия защиты была разработана для обеспечения безопасности информации, являющейся одним из ключевых элементов нашего бизнеса.

- Ответственность за защиту новой системы возложена на Шэрон Джонс. Ее помощником будет Кен Гаррисон. Вы можете обращаться к ним при возникновении любых вопросов, а также при обнаружении возможных нарушений защиты.
- Решения о том, какие функции будут доступны тем или иным сотрудникам, мы принимали на основании нашей текущей политики в отношении информации. Например:
  - Информация о контрактах и особых ценах считается конфиденциальной. Она ни при каких условиях не должна покидать пределов компании.
  - Пределы кредитования клиентов могут устанавливаться только сотрудниками бухгалтерии.
- Все, кто будет работать с системой, получат идентификатор пользователя и пароль. При первом входе в систему, а также каждые 60 дней вы должны будете изменять пароль. Выберите пароль, который вы сможете запомнить, но который не является очевидным. Рекомендации по выбору паролей приведены в форме, которую вы получите вместе с идентификатором пользователя.
- *Не сообщайте свой пароль никому*. Мы хотим, чтобы у вас был доступ ко всем функциям системы, необходимым для нормальной работы. Если вам требуется доступ к информации - обратитесь к Шэрон или Кену. Если вы забыли пароль, Шэрон и Кен безотлагательно помогут установить новый. Никто не должен входить в систему с использованием чужого идентификатора и пароля.
- Возможно, вы знакомы с функцией рабочей станции, позволяющей записывать и воспроизводить набор текста. *Ни в коем случае* не используйте эту функцию для хранения пароля.
- Не оставляйте рабочую станцию подключенной к системе, если вы отходите от рабочего места. Во время обучения вы узнали, как можно временно выйти из системы. Используйте эту возможность, если вам требуется покинуть рабочее место на короткое время. Если вы удаляетесь на длительное время, завершите работу и выйдите из системы с помощью обычной процедуры.

  Выход из системы при уходе с рабочего места особенно важен в помещениях, доступных посторонним людям; к числу таких помещений можно отнести склад, отдел обслуживания клиентов и удаленный торговый офис.
- Несмотря на то, что системный блок - довольно надежное устройство, старайтесь не ударять его и не класть на него посторонние предметы. Панели управления, расположенные на системном блоке, обычно отключены, однако прикасаться к ним не следует. За сохранность системного блока отвечают сотрудники бухгалтерии.

Помните - новая система призвана упростить нашу работу и повысить эффективность нашего бизнеса. Стратегия защиты разработана для того, чтобы помогать вам, а не мешать. Если у вас есть какие-либо вопросы или предложения - вы можете обращаться к Шэрон, Кену или ко мне.

После создания документа, описывающего стратегию защиты, вы можете перейти к планированию групп пользователей.

Планирование для групп пользователей

Первый этап процедуры планирования стратегии защиты - это выбор стратегии компании (т.е. параметров защиты системы в целом). В данном разделе обсуждается второй этап - планирование для групп пользователей, что можно сравнить с выбором стратегии защиты отдела.

Что такое группа пользователей?

Группа пользователей - это группа лиц, работающих с одними и теми же приложениями одинаковым способом. Обычно группа пользователей состоит из сотрудников одного отдела, выполняющих схожие обязанности. Группа пользователей определяется посредством создания профайла группы.

Каковы функции профайла группы?

Профайл группы выполняет в системе следующие две функции:

- **Средство защиты**: Профайл группы задает права доступа к объектам, т.е. определяет круг пользователей, которым разрешено работать с определенными объектами в системе. Профайл группы позволяет задавать права доступа сразу для всех членов группы, а не для каждого пользователя в отдельности.
- **Средство настройки**: Профайл группы можно применять в качестве шаблона для создания профайлов отдельных пользователей. Как правило, параметры большинства членов группы, такие как начальное меню и принтер по умолчанию, совпадают. Эти параметры можно задать в профайле группы и затем скопировать в профайлы пользователей.

Профайлы групп позволяют создать простую, согласованную схему настройки и защиты.

Какие формы вам потребуются?

При планировании защиты для групп пользователей нужны следующие формы:

- Форма Идентификация группы пользователей
- Форма Описание группы пользователей

Примечание: Для каждой группы пользователей в системе потребуется своя собственная форма Описание группы пользователей.

Процедуры заполнения этих форм описаны в следующих разделах:

- Идентификация групп пользователей.
- Планирование для профайлов групп.
- Выбор значений, управляющих входом в систему.
- Выбор значений для ограничения действий пользователя в системе.
- Выбор значений для настройки пользовательской среды.

Идентификация групп пользователей

Прежде чем начать планирование для групп пользователей, вы должны идентифицировать группы пользователей в системе. Это позволит вам спланировать доступ к ресурсам, необходимым этим группам. Идентификацию групп пользователей можно провести достаточно просто. Определите, какие отделы или рабочие группы планируют использовать систему. Посмотрите на диаграмму приложений, которую вы ранее начертили для своих приложений. Проверьте, не существует ли естественных взаимосвязей между рабочими группами и приложениями:

- Можете ли вы выделить основное приложение для каждой рабочей группы?
- Знаете ли вы, какие приложения нужны каждой группе? Какие приложения не потребуются?
- Знаете ли вы, какие группы будет владеть информацией в библиотеках приложений?

Если вы ответили ″Да″ на все эти вопросы, то можете начинать планирование для групп пользователей. Если же вы ответили ″иногда″ или ″возможно″, то вам придется потратить дополнительное время на идентификацию групп пользователей.

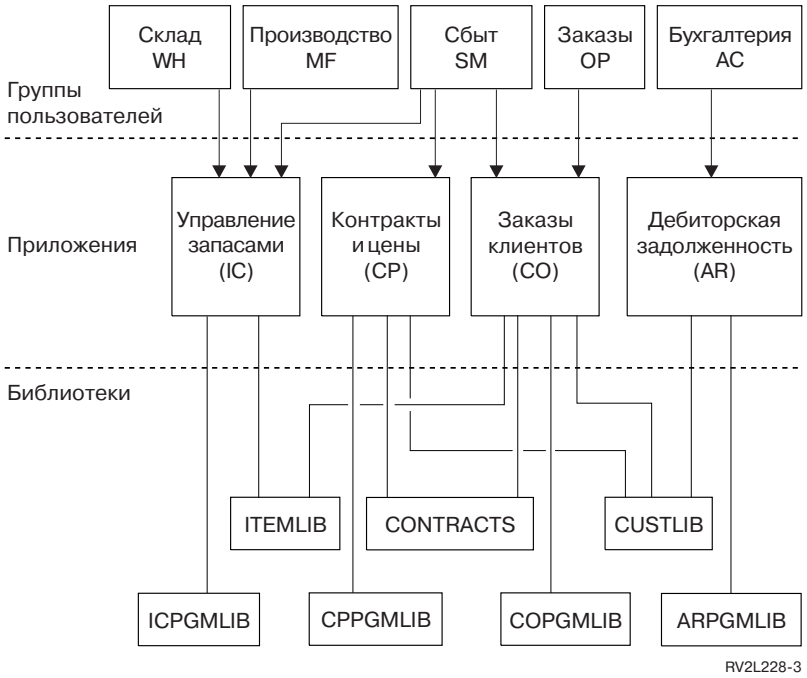
Рекомендуем предварительно ознакомиться с примером.

Примечание: Объединение всех пользователей в одну группу упрощает управление защитой. Однако в некоторых случаях предпочтительнее разбить пользователей на несколько групп.

Обычно легче управлять несколькими профайлами групп, чем предоставлять частные права доступа отдельным профайлам пользователей.

Пример: Идентификация групп пользователей: Если вам нелегко определить, какие приложения применяются той или иной рабочей группой, то вы можете воспользоваться табличной формой, подобной форме Идентификация группы пользователей. Она позволяет составить графическую схему взаимодействия между пользователями и приложениями. Для того чтобы установить, к каким приложениям должны иметь доступ группы пользователей, Шэрон Джонс, например, помимо заполнения формы Идентификация групп пользователей применяет диаграмму приложений.

На рисунке показана диаграмма приложений компании JKL Toys.



Если вы придерживаетесь концепции ″мягкой″ защиты, пометьте буквой X пользователей, которым требуется это приложение. Если вы сторонник ″строгой″ защиты, вам необходимо решить, каким образом пользователи будут получать доступ к приложениям. Если пользователь будет просто просматривать данные в приложении, пометьте его не буквой X, а буквой V (view - просмотр). Если пользователю необходимо вносить изменения в эти данные, пометьте его буквой C (change - изменение). Пользователя, на котором лежит основная ответственность за эти данные, пометьте буквой O (owner - владелец).

Например, в компании JKL Toys приложение Цены и контракты требуется следующим пользователям:

- Отделу сбыта, который устанавливает цены и составляет контракты с клиентами. Сотрудники этого отдела *владеют* информацией о ценах и контрактах.
- Отделу заказов (поступающих от клиентов). Когда сотрудники этого отдела обрабатывают конкретные заказы, количественные соотношения в контракте изменяются. Сотрудникам этого отдела необходимо *изменять* информацию о ценах и контрактах.
- Сотрудникам, обрабатывающим заказы, для планирования своей работы необходимо просматривать информацию о размерах кредита, но они не имеют права изменять ее. Им требуется только *просматривать* файл с информацией о размерах кредита.

Таблица 19. Пример формы Идентификация группы пользователей в компании JKL Toys

Идентификация группы пользователей

Таблица 19. Пример формы Идентификация группы пользователей в компании JKL Toys (продолжение)

Составитель: Шэрон Джонс		Дата: 9/2/99			
		Необходим доступ к приложениям			
Имя пользователя	Отдел	Прил.: CO	Прил.: IC	Прил.: PC	Прил.: AR
Кен Г.	Обработка заказов (OP)	O	C	C	C
Карен Р.	Обработка заказов (OP)	O	C	C	C
Крис Т.	Бухгалтерия (AC)	V		V	O
Сэнди Дж.	Бухгалтерия (AC)	V	C	V	O
Питер Д.	Бухгалтерия (AC)	C		V	O
Рэй У.	Склад (WH)	V	O	V	
Роуз К.	Склад (WH)	V	O	V	
Роджер Т.	Отдел сбыта (SM)	C	C	O	C
Шэрон Дж.	Управляющие (MG)	C	C	C	C

Примечание:

- Если вы планируете установить уровень защиты *Relaxed* ("мягкая защита"), помечайте буквой X приложения, которые требуются пользователям.
- Если вы планируете установить уровень защиты *Average* ("средняя защита"), помечайте буквой A соответствие между пользователями и приложениями.
- Если вы планируете установить уровень защиты *Strict* ("строгая защита"), с помощью букв C (change - изменить), V (view - просмотреть) и O (owner - владелец) определите, *как* будут использоваться приложения.

При подготовке таблицы Шэрон Джонс сделала несколько замечаний:

- Отдел обработки заказов и бухгалтерия предоставляют друг другу копии своих документов. Сегодня этим отделам требуется доступ к одним и тем же приложениям. Тем не менее, однако, они должны быть представлены разными группами, поскольку в будущем, при расширении штата сотрудников, они превратятся в более специализированные подразделения.
- Хотя мы и не разрешаем сотрудникам, обрабатывающим заказы, напрямую вносить изменения в перечень продукции или в контракты, следует учесть, что когда эти сотрудники составляют и заполняют заказы, остатки по счетам изменяются автоматически. Следует ли в будущем установить для них защиту?
- Сотрудники отдела сбыта участвуют во всех этапах производственного процесса и имеют доступ ко всем приложениям. Они устанавливают цены и создают описания выпускаемой продукции. Они находят новых клиентов, хотя бухгалтерия устанавливает ограничения по кредитам. Они отвечают за составление контрактов и за цены.

Определите, какие группы пользователей следует создать в вашей компании. Если вы испытываете затруднения, заполните форму Идентификация группы пользователей.

После добавления пользователей в форму Идентификация группы пользователей вы можете начать планирование профайла группы.

Планирование для профайлов групп

После того как вы определили группы пользователей, можно приступать к планированию профайла для каждой группы. Многие принимаемые вами решения влияют на защиту и на настройку. Например, когда вы задаете начальное меню, вы можете ограничить доступ пользователя к системе только этим меню. Однако при этом необходимо убедиться, что при входе в систему пользователь будет видеть правильное меню.

В качестве примера подготовьте форму Описание группы пользователей для одной группы. После этого вы можете вернуться обратно и заполнить формы для всех остальных групп.

В системе iSeries предусмотрена гибкая система защиты и настройки. Способ планирования, описанный в данном разделе, достаточно удобен для создания профайлов групп и описаний заданий, однако ваш программист или поставщик приложений могут порекомендовать вам другой способ.

Присвоение имен профайлам групп

Профайл группы представляет собой особый тип профайла пользователя, поэтому для упрощения их идентификации в списках и меню рекомендуется присваивать им специальные имена. Для того чтобы все профайлы групп в списке оказались рядом, они должны начинаться с одних и тех же символов, например, GRP (для группы) или DPT (для отдела). При присвоении имен группам пользователей соблюдайте следующие правила:

- Имя группы пользователей может включать до 10 символов.
- Имя может содержать буквы, цифры и специальные символы: знак фунта (#), знак доллара ($), символ подчеркивания (_) и коммерческое ″а″ (@).
- Имя не должно начинаться с цифры.

Примечание: Система присваивает профайлу группы номер, называемый идентификатором группы (*gid*). Обычно идентификатор группы генерируется системой. Однако, если система работает в сети, то вам, возможно, придется самостоятельно присваивать идентификаторы профайлам групп. Выясните это у администратора сети.

Вы должны указать используемое вами соглашение о присвоении имен профайлам групп в соответствующем поле формы Соглашение о присвоении имен. Например, Шэрон Джонс в качестве такого соглашения выбрала DPT. Ниже указано, как она заполнила соответствующий раздел формы Соглашение о присвоении имен.

Таблица 20. Форма Соглашение о присвоении имен в компании JKL Toys: Пример профайла группы

Тип объекта	Соглашение о присвоении имен
Профайлы групп	Имя состоит из букв DPT и сокращенного названия отдела. Текст описания профайла группы содержит полное название отдела.

Определение приложений и библиотек, требующихся группе пользователей

Добавьте группы пользователей (если вы еще не сделали этого) в диаграмму приложений и схему библиотек, которые вы начертили ранее. Эта схема поможет вам определить, какие ресурсы и приложения требуются каждой группе.

В Части 1 формы Описание группы пользователей укажите основное приложение группы, т.е. приложение, которое пользователи группы будут применять наиболее часто. Перечислите другие необходимые группе приложения.

Просмотрите формы Описание приложения и диаграмму приложений и определите, какие библиотеки требуются каждой группе. Согласуйте с разработчиком или поставщиком приложений способы предоставления доступа к этим библиотекам. Наиболее распространены следующие способы:

- Приложение помещает библиотеки в начальный список библиотек пользователя.
- Приложение запускает программу настройки, которая помещает библиотеки в список библиотек пользователя.
- Библиотеки не требуется задавать в списке библиотек. Библиотека всегда указывается самим приложением.

Список библиотек применяется системой для поиска файлов и программ, которые требуются при запуске приложений. **Список библиотек** - это список, в котором система ищет объекты, необходимые пользователю. Список состоит из двух частей:

1. **Системная часть**: определена в системном значении QSYSLIBL и применяется для библиотек OS/400. Настройка по умолчанию для этого системного значения изменяться не должна.
2. **Пользовательская часть**: определяется системным значением QUSRLIBL. Начальный список библиотек, или команд, которые выполняются после входа пользователя в систему, задается описанием задания пользователя. Если у вас есть начальный список библиотек, то он переопределяет системное значение QUSRLIBL. В пользовательскую часть списка библиотек должны быть включены библиотеки приложений.

Использование описания задания

Когда пользователь входит в систему, многие характеристики задания пользователя (параметры вывода на принтер, порядок запуска пакетных заданий, начальный список библиотек) определяются описанием этого задания. Система поставляется с описанием задания с именем QDFTJOBD, которое можно использовать для создания профайлов групп. Однако QDFTJOBD определяет системное значение QUSRLIBL в качестве начального списка библиотек. Если вы хотите, чтобы разные группы пользователей получали при входе в систему доступ к разным библиотекам, вы должны создать уникальные описания заданий для каждой группы.

В форме Описание группы пользователей перечислите все библиотеки, требующиеся данной группе. Если библиотеку следует включить в начальный список библиотек в описании задания группы, отметьте ее имя в этой форме.

Перед тем как выбирать значения для управления входом в систему, ознакомьтесь с примером описания групп пользователей в компании JKL Toy.

Пример: Форма Описание группы пользователей компании JKL Toys: В первой таблице показана 1 часть формы Описание группы пользователей, составленной Шэрон Джонс для отдела продаж и маркетинга. Обратите внимание, что в начальный список библиотек группы не включены библиотеки CONTRACTS и CPPGMLIB. Приложение автоматически добавит их в список библиотек, поэтому добавления этих библиотек в список группы DPTSM не требуется. Когда пользователь выходит из приложения, система удаляет эти библиотеки из списка. Это обеспечивает дополнительную защиту библиотек, так как доступ к ним возможен только через прикладные программы.

Таблица 21. Пример описания группы пользователей компании JKL Toys: Подробное описание

Описание группы пользователей	Часть 1 из 2
Составлено: Шэрон Джонс	Дата: 9/5/99
Имя профайла группы: DPTSM Описание группы: Отдел продаж и маркетинга	
Основное приложение группы: Контракты и цены Перечислите остальные приложения, используемые группой: Управление запасами (для ввода описаний и цен продуктов), Заказы клиентов	
Перечислите все требуемые группе библиотеки. Отметьте (✓) все библиотеки, которые требуется включить в начальный список библиотек группы: • ✓CUSTLIB • ✓ITEMLIB • ✓COPGMLIB • ✓ICPGMLIB • CPPGMLIB • CONTRACTS	

Кроме этого, Шэрон приступила к заполнению формы Описание группы пользователей для складского отдела.

Таблица 22. Описание группы пользователей: Подробное описание

Описание группы пользователей	Часть 1 из 2
Составлено: Шэрон Джонс	Дата: 9/5/99
Имя профайла группы: DPTWH Описание группы: Склад	
Основное приложение группы: Управление запасами Перечислите остальные приложения, используемые группой: нет	
Перечислите все требуемые группе библиотеки. Отметьте (✓) все библиотеки, которые требуется включить в начальный список библиотек группы: • ✓ITEMLIB • ✓ICPGMLIB	

После заполнения 1 части формы Описание группы пользователей вы можете перейти к выбору параметров, влияющих на вход в систему.

Выбор значений, управляющих входом в систему

После того как вы выполните процедуру планирования для профайлов групп, вам необходимо выбрать системные значения, управляющие входом в систему. Эти значения указываются в Части 2 формы Описание группы пользователей. Помните, что данные значения будут скопированы в профайлы пользователей - членов группы. Сначала введите имя выбранного вами профайла группы и краткое текстовое описание группы.

Если вы правильно настроили систему, то в окне Вход в систему пользователям нужно будет ввести только свой идентификатор и пароль. Другие значения, управляющие входом в систему, содержатся в профайлах пользователей.

Пароль

Задайте для профайла группы пароль *NONE. Это не позволит никому войти в систему с помощью профайла группы. Позднее, когда вы будете создавать профайлы пользователей, копируя в них профайл группы, вы сможете установить пароль для каждого пользователя.

Начальная программа и начальная процедура

Перед тем как система выдаст первое меню, выполняется начальная программа пользователя, называемая также **программой входа в систему**. Укажите в профайле группы и имя этой программы, и имя ее библиотеки, даже если эта библиотека входит в начальный список библиотек. Указание обоих имен гарантирует, что система запустит нужную программу и вам не придется беспокоиться о возможных изменениях списка библиотек.

Начальная программа или процедура используется по одной из следующих причин:

- Некоторые приложения используют начальную программу для настройки своей среды.
- Вы хотите, чтобы пользователь запускал только одну программу и никогда не видел меню. Например, в компании JKL Toys сотрудникам, имеющим дело с рабочей станцией на складе, требуется только программа, обрабатывающая прием товаров. Такое ограничение сводит к минимуму риск нарушения защиты на рабочей станции, находящейся в общедоступном месте.

В поле **Ограничение возможностей** укажите для пользователя значение *YES или *PARTIAL. В этом случае пользователь не сможет изменять начальную программу в меню Вход в систему.

Обратитесь к программисту и выясните, требуется ли для ваших приложений начальная программа или процедура.

Начальное меню и библиотека начального меню

Начальное меню, называемое также **первое меню**, - это меню, которое увидит пользователь сразу после того, как войдет в систему. Перед тем как будет показано начальное меню, выполняется начальная программа. Если в начальной программе предусмотрена выдача каких-то меню, то пользователь увидит их до начального меню.

Начальное меню для группы обычно должно быть основным меню главного приложения группы. Укажите имя меню и имя его библиотеки.

Значение *YES, указанное для пользователя в поле **Ограничение возможностей**, запрещает пользователю изменять начальное меню в окне Вход в систему; значение *PARTIAL - напротив, разрешает.

Текущая библиотека

Текущая библиотека называется также **библиотекой по умолчанию**. Когда вы задаете для пользователя текущую библиотеку, происходит следующее:

- Если пользователь создает какие-то объекты, например, программы запросов, система помещает их в текущую библиотеку, если пользователь не указал другую библиотеку.
- Система автоматически добавляет текущую библиотеку в пользовательскую часть списка библиотек. Текущая библиотека может быть включена в начальный список библиотек в описании задания, но это не обязательно.
- Текущая библиотека становится первой библиотекой в пользовательской части списка библиотек. Перед тем как просматривать библиотеки в списке библиотек пользователя, система ищет файлы и программы в текущей библиотеке.
- Если вы не задаете для пользователя текущую библиотеку, то по умолчанию ее роль играет библиотека QGPL (библиотека общего назначения).

Рекомендации

Текущая библиотека особенно важна, если вы планируете работать с лицензионной программой IBM Query для iSeries или аналогичной программой. Ниже приведены некоторые рекомендации:

- Создайте для всех членов группы общую библиотеку. Помещайте все программы запросов и файлы данной группы в эту библиотеку. Присвойте ей такое же имя, что и профайлу группы, и сделайте ее текущей библиотекой группы.
- Каждому пользователю, который будет работать с программой Query, выделите персональную библиотеку. Присвойте ей имя профайла пользователя. Назначьте ее текущей библиотекой в профайлах членов группы, но не в профайле группы.

Укажите выбранные вами значения, управляющие входом в систему, в полях Части 2 формы Описание пользователя.

После этого вы можете выбрать значения для ограничения действий пользователя в системе.

Выбор значений для ограничения действий пользователя в системе

После того как в Части 2 формы Описание группы пользователей вы задали значения, управляющие входом в систему, вы должны решить, как ограничивать действия пользователей в системе. Рекомендуется вводить эти ограничения по следующим причинам:

- Во избежание случайного повреждения информации сотрудниками, которые захотят поэкспериментировать с командами CL.
- С целью ограничить доступные пользователю ресурсы определенным набором приложений и функций.

- С целью создать простую среду, в которой не будет ненужных опций.

Возможности пользователя в системе определяются многими факторами, в частности:
- Приложением
- Системными значениями
- Защитой ресурсов
- Профайлами групп
- Профайлами пользователей
- Описаниями заданий

Возможность пользователя отменять и изменять принятые вами решения зависит от значений, указанных в полях **Ограничение возможностей** и **Класс пользователя** профайла пользователя.

Ограничение возможностей

Поле **Ограничение возможностей** называется **Ограниченное использование командной строки**. Вы можете определить, будет разрешено ли пользователям изменять значения в меню Вход в систему, вводить команды и изменять программу обработки клавиши Attention. В поле Ограничение возможностей можно задавать следующие значения: *YES (строгие ограничения), *PARTIAL (средние ограничения) или *NO (нет ограничений). В приведенной ниже таблице объясняется, что разрешает каждое из этих значений:

Таблица 23. Функции, которые разрешено выполнять для данного типа ограничений:

Тип ограничений	Изменение начальной программы	Изменение начального меню	Изменение текущей библиотеки	Изменение программы Attention	Ввод команд
*YES	Нет	Нет	Нет	Нет	Некоторые[1]
*PARTIAL	Нет	Да	Нет	Нет	Да
*NO	Да	Да	Да	Да	Да

1 Разрешено выполнять следующие команды: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG и STRPCO. Пользователь не может нажимать клавишу F9 для просмотра командной строки из любого меню или окна Операционная поддержка.

Класс пользователя

Класс пользователя, называемый также **тип пользователя**, определяет, какие опции системных меню и меню Операционная поддержка видит пользователь. Кроме того, класс пользователя определяет, какие системные функции разрешено выполнять пользователю, если вы не задаете список прав доступа в поле **Специальные права доступа**.

Рекомендации по установке ограничений возможностей и классов пользователей

Большинству пользователей не нужен доступ к командам CL и системным функциям. Им достаточно информации и возможностей меню Операционная поддержка. Следующие рекомендации позволяют ограничить доступ пользователей только к тем системным ресурсам, которые им необходимы:
- Во всех профайлах групп в поле **Ограничение возможностей** укажите *YES, а в поле *Класс пользователя* - *USER.
- Если отдельным пользователям необходимо выполнять системные функции, переопределите для них эти значения.
- Убедитесь в том, что ваши меню позволяют переходить от одного приложения к другому, если это необходимо пользователям.

После того как в Части 2 формы Описание группы пользователей вы задали класс пользователя и ограничения возможностей пользователей, вы можете выбирать значения для настройки пользовательской среды.

Выбор значений для настройки пользовательской среды

После того как в Части 2 формы Описание группы пользователей вы задали ограничения на действия пользователей в системе, вы можете указать значения для настройки операционной среды пользователя. В профайле пользователя для этого предусмотрено множество полей. Они определяют, например, какой принтер использовать, куда отправлять сообщения, с каким приоритетом запускать задания. В большинстве этих полей рекомендуется указывать значения по умолчанию. Несколько полей описаны ниже.

- **Описание задания и библиотека описания задания**: Эти поля указывают системе, какое описание задания она должна использовать при входе пользователя в систему. Описание задания содержит начальный список библиотек. Для каждой группы пользователей должно существовать свое описание задания с тем же именем, что и профайл группы. Описания заданий обычно помещаются в библиотеку QGPL.
- **Принтер и очередь вывода**: Любой вывод на принтер, создаваемый пользователем, направляется на принтер, указанный в профайле этого пользователя, если только конкретное задание печати не отправляет его на другой принтер. Члены одной группы обычно находятся рядом друг с другом и печатают на одном и том же принтере. Вы можете указать этот принтер в профайле группы и затем скопировать это значение в профайлы всех пользователей этой группы. Принтер пользователя называется также **принтером по умолчанию**.

  Прежде чем вывод на принтер будет напечатан, он попадает в очередь вывода. Обычно для каждого принтера задается своя очередь вывода с тем же именем. Если для очереди вывода задать значение *DEV, то система будет использовать очередь вывода данного принтера.

  Укажите имя описания задания и имя его библиотеки, а также принтер по умолчанию и очередь вывода в полях формы Описание группы пользователей.
- **Настройка интерфейса Операционная поддержка**: В поставляемой системе набор меню Операционная поддержка - это программа обработки клавиши Attention для каждого пользователя. Когда пользователь нажимает клавишу Attention, он видит меню Операционная поддержка (ASSIST). Если в ваших приложениях уже применяется другая программа обработки клавиши Attention, вы должны задать другой способ доступа пользователей к меню Операционная поддержка:
  - Добавьте ссылку на меню Операционная поддержка в виде опции в меню вашего главного приложения, либо воспользуйтесь командами `GO ASSIST` или `CALL QEZAST`.
  - Предложите пользователям вводить `GO ASSIST` в командной строке.

Если в профайле пользователя в поле **Ограничение возможностей** указано значение *YES, то пользователь не сможет открыть меню с помощью команды GO. Вам необходимо предусмотреть другой способ доступа к меню ASSIST.

Рекомендуем ознакомиться с примером выбора значений в форме Описание группы пользователей в компании JKL Toys.

Для завершения этих этапов планирования вы должны:

- Заполнить форму Описание группы пользователей для всех групп пользователей в вашей компании.
- Описать способ присвоения имен группам пользователей в форме Соглашение о присвоении имен.
- Добавить группы пользователей в диаграмму приложений и библиотек.

После выполнения всех этих задач вы можете приступить к планированию профайлов отдельных пользователей.

Пример: Форма описания групп пользователей компании JKL Toy—Часть 2: Во время подготовки описания группы пользователей, включающей сотрудников отдела продаж и маркетинга, Шэрон Джонс сделала ряд заметок, относящихся к отделу продаж и маркетинга, а также к складу:

- Сотрудники отдела сбыта будут интенсивно работать с программой Query. Для каждого пользователя следует создать собственную библиотеку. Работникам склада можно предоставить общую библиотеку для всей группы.
- Для сотрудников склада, работающих на приеме товаров, нужно настроить начальную программу, а не начальное меню.

Шэрон подготовила 2 часть Описания групп пользователей для двух отделов.

Таблица 24. Пример описания группы пользователей компании JKL Toy: отдел продаж и маркетинга

Имя поля	**Рекомендованное значение**	**Выбранный вариант**
Имя профайла группы (Пользователь)		DSTSM
Пароль	*NONE	*NONE
Класс пользователя (Тип пользователя)	*USER	*USER
Текущая библиотека (Библиотека по умолчанию)	*совпадает с именем профайла группы*	(оставить пустым для группы, заполнить для отдельных профайлов)
Начальная программа (программа входа в систему)		
Библиотека начальной программы		
Начальное меню (первое меню)		CPMAIN
Библиотека начального меню		CPMAINLIB
Ограничить возможности (Ограничить использование командной строки)	*YES	*PARTIAL
Описание (Описание пользователя)		Отдел продаж и маркетинга
Описание задания	*совпадает с именем профайла группы*	DPTSM
Библиотека описания задания		QGPL
Имя профайла группы (Группа пользователей)	*NONE[1]	*NONE
Печатающее устройство (Принтер по умолчанию)		PRT03
Очередь вывода	*DEV	*DEV

Таблица 25. Пример описания группы пользователей компании JKL Toy: склад

Имя поля	**Рекомендованное значение**	**Выбранный вариант**
Имя профайла группы (Пользователь)		DPTWH
Пароль	*NONE	*NONE
Класс пользователя (Тип пользователя)	*USER	*USER
Специальная среда		
Текущая библиотека (Библиотека по умолчанию)	*совпадает с именем профайла группы*	DPTWH
Начальная программа (программа входа в систему)		
Библиотека начальной программы		
Начальное меню (первое меню)		ICMAIN
Библиотека начального меню		ICPGMLIB

Таблица 25. Пример описания группы пользователей компании JKL Toy: склад (продолжение)

Имя поля	Рекомендованное значение	Выбранный вариант
Ограничить возможности (Ограничить использование командной строки)	*YES	*YES
Описание (Описание пользователя)		Склад
Описание задания	*совпадает с именем профайла группы*	DPTWH
Библиотека описания задания		QGPL
Имя профайла группы (Группа пользователей)	*NONE[1]	*NONE
Печатающее устройство (Принтер по умолчанию)		PRT04
Очередь вывода	*DEV	*DEV

1 В профайле группы следует указать имя профайла *NONE. Профайл группы не может быть членом другой группы.

Теперь можно перейти к планированию профайлов отдельных пользователей.

Планирование профайлов пользователей

Теперь, когда вы определили общую стратегию защиты и спланировали группы пользователей, вы можете приступить к планированию профайлов отдельных пользователей.

Какие формы вам потребуются?

Для планирования профайлов пользователей предназначены следующие формы:

- Форма Профайл пользователя
- Форма Полномочия в системе

Кроме того, вам потребуется информация из следующих заполненных форм:

- Форма Определение группы пользователей
- Форма Соглашения о присвоении имен
- Диаграмма вашего приложения

Присвоение имен профайлам пользователей

Имя пользовательского профайла - это имя, под которым пользователь известен системе. Оно вводится пользователем в поле **ИД пользователя** в меню Вход в систему. Любые действия пользователя и создаваемый им вывод на принтер связаны с именем его профайла.

При выборе имени профайла учтите следующие ограничения:

- Имя пользовательского профайла может включать до 10 символов. В некоторых вариантах соединений длина ИД пользователя ограничивается 8 символами.
- Имя может содержать буквы, цифры и специальные символы: знак фунта (#), знак доллара ($), символ подчеркивания (_) и коммерческое ″a″ (@). Имя не может начинаться с цифры или с символа подчеркивания (_).
- Строчные и прописные буквы в имени пользовательского профайла не различаются. При вводе буквенно-цифровых символов в нижнем регистре они автоматически преобразуются в верхний регистр.
- Во всех окнах и списках имена профайлов располагаются в алфавитном порядке.
- Все профайлы, определенные фирмой IBM, начинаются с буквы Q. Для того чтобы отличать от них свои профайлы, не присваивайте своим профайлам имена, начинающиеся с буквы Q.

Рекомендации

Один из способов выбора имен пользовательских профайлов состоит в том, чтобы указывать первые семь букв фамилии пользователя и затем первую букву его имени. Ниже приведены примеры имен, которые Шэрон Джонс присвоила профайлам сотрудников JKL Toys:

Таблица 26. Форма Соглашение о присвоении имен в JKL Toys: Пример пользовательского профайла

Имя пользователя	**Имя пользовательского профайла**
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jones, Sharon	JONESS

Такие имена профайлов легко запомнить, кроме того, все списки будут упорядочены по фамилиям пользователей в алфавитном порядке.

Предположим, что Шэрон Джонс планирует применять этот способ присвоения имен профайлам. Она заполнила соответствующий раздел формы Соглашения о присвоении имен.

Таблица 27. Форма Соглашение о присвоении имен в JKL Toys: Пример пользовательского профайла

Тип объекта	**Соглашение о присвоении имен**
Пользовательские профайлы	Используются первые семь букв фамилии пользователя и первая буква его имени. Описание пользовательского профайла состоит из фамилии и имени пользователя.

В форме Соглашения о присвоении имен опишите способ выбора имен для пользовательских профайлов; затем вы можете определить, кто будет отвечать за системные функции, и выбрать значения для каждого пользователя.

Определение пользователей, ответственных за выполнение системных функций

При планировании профайлов отдельных пользователей вы должны сначала разграничить полномочия в системе. Для обеспечения эффективной работы системы вам необходимо выбрать пользователей, которые будут регулярно выполнять функции по управлению и обслуживанию системы. Им необходимо предоставить права на выполнение команд и системных функций.

В разделе Выбор значений для ограничения действий пользователя в системе обсуждается, как управлять доступом пользователей к системным функциям с помощью полей **Класс пользователя** и **Ограничение возможностей**. В большинстве случае вы не должны разрешать пользователям выполнять системные функции (задайте для этого класс пользователя *USER и ограничение возможностей *PARTIAL или *YES). Однако для некоторых пользователей следует сделать исключение, чтобы работа системы была более эффективной.

В приведенной ниже таблице перечислены некоторые важные задачи управления системой. Кроме того, в ней указано, какие специальные права доступа и класс пользователя вы можете присвоить пользователям, ответственным за выполнение этих задач. Данный список поможет вам определить, каким пользователям в системе необходимы специальные права доступа. Однако не следует рассматривать его как единственный инструмент планирования работы и обслуживания вашей системы. В таблице указываются класс пользователя и специальные права доступа, которые работают в большинстве систем. Какие именно права вы будете предоставлять конкретным пользователям - зависит от вашей системы.

Если вы указываете в профайле класс пользователя, отличный от *USER, то пользователь автоматически получает определенный набор специальных прав на выполнение системных функций. Вы можете предоставить пользователю специальные права, которые отличаются от тех, которые вы задали в поле Класс пользователя, но делать это необязательно.

Таблица 28. Полномочия в системе, Класс пользователя, Специальные права доступа

Системная функция[1]	**Описание**	**Необходимый класс пользователя**[2]	**Необходимые специальные права доступа**[3]
Системные операции	Управление выводом на принтер, ответ на системные сообщения, контроль за регулярными операциями, выполнение загрузки начальной программы (IPL).	*SYSOPR	*JOBCTL
Системные сервисные функции	Выполнение системных сервисных функций, таких как составление расписания автоматической очистки и контроль за использованием дисков.	*SYSOPR	*JOBCTL
Резервное копирование системы	Регулярное сохранение библиотек приложений, системных библиотек и информации о защите. Эти функции подробно описаны в разделе Резервное копирование и восстановление Information Center.	*SYSOPR	*SAVSYS
Администрирование профайлов	Добавление новых и обслуживание существующих профайлов пользователей.	*SECADM	*SECADM
Управление защитой ресурсов	Работа с правами доступа к объектам в системе.	*SECOFR	*ALLOBJ
Обслуживание программ	Установка временных изменений программ (PTF) для поставляемых фирмой IBM библиотек. Внесение изменений в библиотеки приложений.	*SECOFR	*ALLOBJ
Контроль за действиями в системе	Настройка функции контроля за действиями. Выбор событий, пользователей и объектов, которые необходимо контролировать.		*AUDIT [4]
Конфигурация системы	Добавление, изменение и удаление устройств из системы.		*IOSYSCFG [5]

1 Для пользователей, ответственных за выполнение этих функций, в поле Ограничения возможностей укажите значение *NO.

2 В таблице указан минимальный класс пользователя, необходимый для доступа к командам и опциям меню, предназначенным для выполнения указанной функции. Возможно, что в вашей системе для доступа к объектам могут потребоваться дополнительные права.

3 Эти права доступа необходимы для запуска заданий. Дополнительные специальные права может предоставить класс пользователя.

4 Для специальных прав доступа *AUDIT нет соответствующего класса пользователя. Специальные права доступа *AUDIT включены в класс пользователя *SECOFR. Возможно, однако, что пользователю, который будет выполнять функцию контроля, другие права класса *SECOFR не потребуются. По этой причине укажите права доступа *AUDIT отдельно для каждого пользователя, ответственного за выполнение функции контроля за действиями в системе.

5 Для специальных прав доступа *IOSYSCFG нет соответствующего класса пользователя. Специальные права доступа *IOSYSCFG включены в класс пользователя *SECOFR. Права доступа *IOSYSCFG необходимо указывать только для пользователей, которые должны настраивать систему. При этом они смогут создавать линии, контроллеры и устройства или настраивать TCP/IP. Возможно, однако, что пользователю, который будет выполнять настройку системы, другие права класса *SECOFR не потребуются.

Рекомендации

Воспользуйтесь этой таблицей для выбора лиц, которые должны будут выполнять системные функции. Вы должны предоставить не менее чем двум пользователям права на управление защитой системы и еще двум - права на управление операциями и резервным копированием.

В качестве инструмента управления и контроля воспользуйтесь формой Полномочия в системе. Контролируйте всех пользователей, которым предоставлены специальные права доступа, и следите, для чего они используют эти права.

Перед тем как выбрать значения для каждого пользователя, ознакомьтесь с примером, в котором показано, как Шэрон Джонс определяет полномочия пользователей.

Пример: Форма Ответственные за работу системы компании JKL Toy: Ниже показан пример списка ответственных за работу системы, составленного Шэрон Джонс:

Таблица 29. Пример: Форма Ответственные за работу системы компании JKL Toy

Кто ваш системный администратор? Шэрон Джонс Кто заместитель системного администратора?Кен Гаррисон			
Имя профайла	Имя пользователя	Класс	Комментарии
JONESS	Шэрон Джонс	*SECOFR	Шэрон - основной администратор системы.
HARRISOK	Кен Гаррисон	*SECOFR	Кен является заместителем Шэрон по вопросам управления системой.
JOHNSONS	Сэнди Джонсон	*SYSOPR	Сэнди отвечает за работу системы и резервное копирование.
ROGERSK	Карен Роджерс	*SYSOPR	Карен будет помогать Сэнди в вопросах поддержки системы и резервного копирования.
WILLISR	Роуз Виллис	*SYSOPR	Роуз будет управлять работой системы во второй смене.

После заполнения формы Ответственные за работу системы вы можете перейти к выбору значений для каждого пользователя.

Выбор значений для каждого пользователя

После того как вы определили полномочия пользователей в системе, вы можете задавать значения для каждого пользователя. Спланировав профайлы групп в качестве шаблонов для профайлов пользователей, вы уже сделали основную часть работы. Для того чтобы правильно включить пользователя в группу и определить, чем он отличается от других пользователей в группе, воспользуйтесь формой Профайл пользователя. Вы должны заполнить в качестве примера форму Профайл пользователя для одной группы пользователей, а затем вернуться обратно и составить формы Профайл пользователя для любого числа дополнительных групп пользователей.

В верхней строке формы Профайл пользователя укажите имя профайла группы и другую информацию описательного характера.

Пример: Описание формы Профайл пользователя компании JKL Toys

Так Шэрон Джонс заполнила верхнее поле формы Профайл пользователя.

Таблица 30. Форма Профайл пользователя компании JKL Toys: пример описания

Форма Профайл пользователя		
Составитель: Шэрон Джонс		Дата: 9/5/99
Имена профайлов группы: DPTOP		
Владелец созданных объектов:	Права доступа группы к создаваемым объектам:	

Таблица 30. Форма Профайл пользователя компании JKL Toys: пример описания (продолжение)

Тип прав доступа группы:

Определение значений для членов группы

В форме Профайл пользователя укажите имя профайла и описание (имя пользователя) каждого члена группы. Порядок определения других параметров для членов группы описывается ниже.

Помните, что профайл группы - это шаблон для профайлов пользователей. В форме Профайл пользователя необходимо задавать только те параметры, которые различаются для разных членов группы.

- **Присвоение паролей**: Самый простой способ присвоения паролей заключается в том, чтобы указать в качестве пароля имя профайла. Затем вы можете потребовать смену пароля при первом входе пользователя в систему, указав срок действия пароля. В разделе Установка срока действия пароля описано, как это делать автоматически при копировании профайла группы. Если вы именно так и собираетесь делать, то задавать список паролей в форме Профайл пользователя не нужно.
- **Класс пользователя и ограничения возможностей**: Откройте форму Полномочия в системе и посмотрите, для каких членов группы необходимо задать иные значения параметров **Класс пользователя** и **Ограничение возможностей**. Укажите для этих пользователей соответствующие значения в их формах Профайл пользователя.
- **Определение других параметров**: Проверьте, нужно ли указывать для данного пользователя значения, отличающиеся от тех, что заданы для данной группы в форме Описание группы пользователей. Поля **Класс пользователя** и **Ограничение возможностей** расположены в начале этой формы, поскольку для некоторых членов группы содержащаяся в них информация может часто меняться. Составьте список других полей, содержащих изменяемые параметры для членов данной группы.

Для того чтобы закончить данный этап планирования, выполните следующие действия:

- Полностью заполните форму Выбор системных значений.
- Опишите способ присвоения имен профайлам пользователей в форме Соглашения о присвоении имен.
- Подготовьте формы Профайл пользователя для всех групп пользователей вашей фирмы.

Перед тем как планировать защиту ресурсов, рекомендуется ознакомиться с примером информации, которую Шэрон Джонс применяет для отдельных пользователей.

Пример: Форма Описание профайла пользователя компании JKL Toy: В компании JKL Toy сотрудники склада, работающие на приеме товаров, могут использовать только одну программу. Шэрон ограничила их возможности в связи с тем, что к рабочим станциям, установленным на складе, легко могут получить доступ посторонние лица. Для работников склада установлена начальная программа и не установлено начальное меню. В отделе обработки заказов установлено два локальных принтера; кроме того, один принтер находится в удаленном торговом офисе. В связи с этим Шэрон настроила для некоторых пользователей принтер, отличный от выбранного для всех остальных членов группы.

Ниже показана форма Описание профайла пользователя, заполненная Шэрон для склада и для отдела обработки заказов компании JKL Toy. Обратите внимание на то, что заполнены только те поля, которые отличаются от соответствующих полей профайла группы.

Таблица 31. Пример описания профайла пользователя компании JKL Toy: склад

Имена профайлов групп: DPTWH					
Добавьте запись для каждого члена группы:					
Профайл пользователя	**Описание**	**Класс пользователя**	**Ограничение возможностей**	**Начальная программа/ библиотека**	**Начальное меню/ библиотека**
WILLISR	Виллис Роуз	*SYSOPR	*NO		

Таблица 31. Пример описания профайла пользователя компании JKL Toy: склад (продолжение)

WAGNERR	Вагнер Рей			ICRCPT/ICPGMLIB	нет
AMESJ	Эмис Дженис			ICRCPT/ICPGMLIB	нет
FOSSJ	Фосс Джулия				
WOODBURC	Вудберт Кэрол				

Таблица 32. Пример описания профайла пользователя компании JKL Toy: отдел обработки заказов

Имена профайлов групп: DPTOP				
Добавьте запись для каждого члена группы:				
Профайл пользователя	**Описание**	**Класс пользователя**	**Ограничение возможностей**	**Принтер**
HARRISOK	Гаррисон Кен	*SECOFR	*NO	PRT05
RICHARDK	Ричардс Карен			
UNGERJ	Унгер Джефф			PRT04
BELLB	Белл Брэд			PRT04

После этого вы можете перейти к планированию защиты ресурсов.

Планирование защиты ресурсов

Перед планированием защиты ресурсов завершите планирование защиты пользователей. Настройка защиты ресурсов описана в разделе ″Настройка защиты ресурсов″.

При настройке системных значений и создании пользовательских профайлов вы определили список сотрудников, у которых есть доступ к системе (т.е. пользователей системы). Цель защиты ресурсов состоит в том, чтобы определить перечень операций, которые пользователи смогут выполнять после входа в систему. Защита ресурсов обеспечивает следующие свойства информации:

- Конфиденциальность (защита от несанкционированного доступа)
- Целостность (защита от несанкционированного изменения)
- Доступность (защита от случайного или преднамеренного повреждения)

Процедуры защиты ресурсов зависят от того, занимается ли ваша компания самостоятельной разработкой приложений или приобретает уже готовые. В первом случае требования защиты должны быть учитываться программистом при проектировании приложения. Во втором случае эти требования должны быть согласованы со средствами защиты, предусмотренными разработчиком приложения. Описанные здесь методы помогут вам в обоих случаях.

В этом разделе описан общий подход к планированию защиты ресурсов. Продемонстрированы основные средства защиты и способы их применения. Применение этих средств зависит от конкретной среды и применяемого набора приложений. При планировании защиты ресурсов в каждом конкретном случае проконсультируйтесь с разработчиками приложения.

Информация, связанная с планированием защиты ресурсов, приведена в следующих разделах:

- Определение защищаемых ресурсов
- Основные сведения о типах прав доступа
- Планирование защиты библиотек приложений
- Выбор владельца для библиотек и объектов
- Объединение объектов в группы
- Защита вывода на принтер

- Защита рабочих станций
- Обзор рекомендаций по защите ресурсов
- Планирование установки приложений

Необходимые формы

Напечатайте следующие формы и ознакомьтесь с приведенными в этом разделе инструкциями по их заполнению. Повторите процедуру планирования защиты для каждого приложения.

Таблица 33. Формы планирования защиты ресурсов

Название формы	**Число копий**
Список прав доступа	Несколько
Защита рабочих станций и вывода на принтер	Одна

Уже существующие формы, которые необходимо дополнить:

Таблица 34. Формы, подлежащие изменению

Название формы	**Составлено:**
Описание библиотеки	Создание описаний библиотек
Описание группы пользователей	Планирование групп пользователей

Уже существующие формы, информация которых вам потребуется:

Таблица 35. Формы планирования, необходимые для защиты ресурсов

Название формы	**Составлено:**
Описание библиотеки	Создание диаграммы приложений и Идентификация групп пользователей
Описание приложения	Создание описаний приложений
Описание пользовательского профайла	Настройка профайлов отдельных пользователей
Описание группы пользователей	Планирование групп пользователей
Ответственные за работу системы	Определение ответственных за работу системы
Планирование физической защиты	Планирование физической защиты

Определение защищаемых ресурсов

Планирование защиты ресурсов должно начинаться с определения защищаемых объектов. Система iSeries обеспечивает гибкую настройку защиты ресурсов. Вы можете защитить наиболее важные ресурсы именно так, как хотите. Но учтите, что защита ресурсов - это дополнительная нагрузка на систему. Например, при каждой попытке обращения к объекту система должна проверить права доступа пользователя к этому объекту. В связи с этим необходимо выбрать оптимальное соотношение между требованиями к уровню защиты и производительности системы.

Для сведения дополнительной нагрузки на систему к минимуму следуйте следующим рекомендациям:

- Не усложняйте схему защиты сверх необходимости.
- Защищайте только те объекты, которые нуждаются в защите.
- Используйте защиту ресурсов только как дополнение, а не как замену других средств защиты информации, таких как:
  - Ограничение доступа пользователей к меню и приложениям.

– Запрет ввода команд для определенных пользователей (параметр Ограничение возможностей пользовательского профайла).

Начните планирование защиты ресурсов с определения списка защищаемых объектов. Для этого заполните формы Описание приложения или Описание библиотеки.

Используемая форма зависит от способа организации информации в библиотеках.

Вы можете ознакомиться с настройкой защиты ресурсов в вымышленной компании JKL Toys, а также с возможными Типами прав доступа.

Пример: Задачи защиты информации в компании JKL Toys

Шэрон Джонс зафиксировала требования по защите библиотеки с информацией о клиентах (CUSTLIB) в форме Описание библиотеки:

Таблица 36. Пример формы Описание библиотеки компании JKL Toys: Задачи защиты

Форма Описание библиотеки	Часть 1 из 2
Определите требования по защите библиотеки, например, уровень конфиденциальности хранящейся в ней информации:	На данный момент просмотр заказов разрешен все сотрудникам компании. Для сохранения целостности информации необходимо ограничить возможность ее изменения.

Требования по защите приложения Контракты и цены Шэрон зафиксировала в соответствующей форме Описание приложения.

Таблица 37. Пример формы Описание приложения компании JKL Toys: Задачи защиты

Описание приложения	Часть 1 из 2
Определите требования по защите библиотеки, например, уровень конфиденциальности хранящейся в ней информации:	Информация о контрактах и особых ценах является конфиденциальной. Просмотр и изменение информации разрешен только нескольким лицам: • Сотрудники и менеджеры отдела продаж и маркетинга должны иметь возможность создания, изменения и анализа контрактов. Они используют как файлы, так и программы. • Сотрудники отдела обработки заказов изменяют контракты и просматривают цены неявно при вводе и обслуживании заказов. Им запрещен просмотр информации о контрактах и ценах, за исключением просмотра при вводе или изменении заказа.

Запишите информацию о защите приложения в форме Описание приложения или Описание библиотеки. Теперь вы можете ознакомиться с описанием различных типов прав доступа, которые можно применять при планировании защиты ресурсов.

Основные сведения о типах прав доступа

Перед планированием типов прав доступа вы должны определить список защищаемых ресурсов и заполнить формы описания библиотек. Для защиты ресурсов необходимо определить, какие операции пользователи должны выполнять над объектами системы.

Права доступа определяют, какие операции пользователь может выполнять над определенным системным объектом. Например, у пользователя могут быть права доступа на просмотр или на изменение какой-либо информации в системе. Система допускает несколько различных типов доступа. Эти типы прав доступа объединены в категории, называемые **системными правами доступа**. Обычно системных прав доступа

достаточно для описания прав доступа любого пользователя к любому объекту. Системные права доступа и их значение для файлов и программ перечислены в следующей таблице.

Примечание: Эти таблицы полезно иметь под рукой при планировании прав доступа.

Таблица 38. Системные права доступа для файлов и программ

Права доступа	Разрешенные операции с файлами	Запрещенные операции с файлами	Разрешенные операции с программами	Запрещенные операции с программами
*USE	Просмотр информации файла.	Изменение или удаление любой информации в файле. Удаление файла.	Запуск программы.	Изменение или удаление программы.
*CHANGE	Просмотр, изменение или удаление записей файла.	Удаление или очистка всего файла.	Изменение описания программы.	Изменение или удаление программы.
*ALL	Изменение или удаление файла. Добавление, изменение или удаление записей файла. Предоставление прав доступа к файлу другим пользователям.	Нет	Создание, изменение или удаление программы. Предоставление прав доступа к программе другим пользователям.	Изменение владельца программы, если использует принятые права доступа.
*EXCLUDE[1]	Нет	Любое обращение к файлу.	Нет	Любое обращение к программе.
1 Права доступа *EXCLUDE имеют наивысший приоритет и переопределяют как общие права доступа, так и права доступа группы.				

Основные сведения о взаимодействии прав доступа к объекту и прав доступа к библиотеке объекта

Для упрощения схемы защиты рекомендуется планировать защиту на уровне библиотек. Значение системных прав доступа для библиотек показано в следующей таблице:

Таблица 39. Системные права доступа для библиотек

Права доступа	Разрешенные операции	Запрещенные операции
*USE	• Для объектов в библиотеке - все операции, разрешенные правами доступа к самим объектам. • Для библиотеки - просмотр описаний.	• Добавление в библиотеку новых объектов. • Изменение описания библиотеки. • Удаление библиотеки.
*CHANGE	• Для объектов в библиотеке - все операции, разрешенные правами доступа к самим объектам. • Добавление в библиотеку новых объектов. • Изменение описания библиотеки.	• Удаление библиотеки.

Таблица 39. Системные права доступа для библиотек (продолжение)

Права доступа	Разрешенные операции	Запрещенные операции
*ALL	• То же, что *CHANGE. • Удаление библиотеки. • Предоставление другим пользователям прав доступа к библиотеке.	• Нет

Кроме того, важно взаимодействие прав доступа к объекту и к его библиотеке. Примеры прав доступа к объекту и к библиотеке, необходимые для выполнения некоторых действий, приведены в следующей таблице:

Таблица 40. Взаимодействие прав доступа к объекту и к его библиотеке

Тип объекта	Операции	Необходимые права доступа к объекту	Необходимые права доступа к библиотеке
Файл	Изменение данных	*CHANGE	*USE
Файл	Удаление файла	*ALL	*USE
Файл	Создание файла	*ALL	*CHANGE
Программа	Запуск программы	*USE	*USE
Программа	Изменение (повторная компиляция) программы	*ALL	*CHANGE
Программа	Удаление программы	*ALL	*USE

Права доступа к каталогам действуют аналогично правам доступа к библиотекам. Для доступа к объекту необходимы права доступа ко всем каталогам, в которых он находится.

Следующий этап - планирование защиты библиотек приложений.

Планирование защиты библиотек приложений

Перед планированием защиты библиотек приложений вы должны определить защищаемые ресурсы. Сначала выполните перечисленные ниже действия для одной из библиотек приложений. Если файлы и программы в вашей системе хранятся в разных библиотеках, выберите ту библиотеку, в которой хранятся файлы. Затем повторите эту процедуру для всех остальных библиотек.

Просмотрите информацию о приложениях и библиотеках, указанную в следующих формах и диаграммах:

- Описание приложения
- Описание библиотеки
- Описание группы пользователей (для всех групп, которым нужен доступ к выбранной библиотеке)
- Диаграмма приложений, библиотек и групп пользователей

Определите, какие группы и как будут работать с информацией, хранящейся в выбранной библиотеке.

Определение содержимого библиотеки

В библиотеках приложений хранятся следующие объекты, необходимые для работы приложений:

- Файлы данных
- Области данных и очереди сообщений
- Программы
- Файлы сообщений

- Команды
- Очереди вывода

Большая часть из перечисленных объектов, за исключением файлов и очередей вывода, не требует защиты. Обычно они содержат небольшие объемы данных в формате приложения, которые трудно расшифровать вне его. Для просмотра списка имен и описаний всех объектов, хранящихся в библиотеке, введите команду Показать библиотеку. Например, для просмотра содержимого библиотеки CONTRACTS введите следующую команду: `DSPLIB LIB(CONTRACTS) OUTPUT(*PRINT)`

Следующий этап - определение общих прав доступа к приложениям и библиотекам.

Определение общих прав доступа к библиотекам приложений

С точки зрения защиты **общий** объект - это объект, доступный любому пользователю, который может войти в систему. **Общие права доступа** - это права доступа к объекту, предоставляемые пользователю в том случае, если права доступа данного пользователя к этому объекту не были заданы явно. Кроме указания общих прав доступа к объектам, уже находящимся в библиотеке, можно задать общие права доступа по умолчанию для новых объектов. Для этого задайте параметр библиотеки **Права доступа к новым объектам (CRTAUT)**. Обычно общие права доступа к объектам библиотеки и к новым объектам совпадают.

В пределах всей системы права доступа к новым объектам по умолчанию задаются системным значением QCRTAUT (Права доступа к новым объектам). По умолчанию системное значение QCRTAUT равно *CHANGE. Изменять QCRTAUT не рекомендуется, поскольку от него зависят многие системные функции. Системное значение QCRTAUT применяется в тех случаях, если в параметре Права доступа к новым объектам (CRTAUT) указано значение *SYSVAL.

Для упрощения схемы защиты и достижения максимальной производительности рекомендуется по возможности изменять общие, а не частные права доступа. Для определения оптимальных общих прав доступа к библиотеке необходимо ответить на следующие вопросы:

- Необходим ли всем пользователям системы доступ к большинству объектов библиотеки?
- Какой тип доступа к объектам библиотеки нужен большинству пользователей системы?

Принятое решение должно соответствовать большинству пользователей и большей части информации. Затем можно будет определить исключения. Планирование защиты ресурсов часто происходит циклически. После определения прав доступа к конкретным объектам иногда возникает необходимость изменить общие права доступа. Для определения оптимального варианта проверьте несколько сочетаний общих и частных прав доступа к объектам и библиотекам.

Достаточные права доступа

Обычно прав доступа *CHANGE к объектам и *USE к библиотеке достаточно для большинства приложений. Для того чтобы проверить это применимость этого правила для конкретного приложения, задайте его разработчикам следующие вопросы:

- Удаляет ли приложение какие-либо объекты из библиотеки? Очищаются ли какие-либо файлы? Добавляются ли к файлам новые элементы? Для удаления объекта и добавление элемента в файл нужны права доступа *ALL.
- Создает ли приложение какие-либо объекты в библиотеке? Для создания объектов нужны права доступа *CHANGE к библиотеке.

Вы можете ознакомиться с примером выбора прав доступа к объектам. Следующий этап - Определение общих прав доступа к библиотекам программ.

Пример: Форма Описание библиотеки компании JKL Toy:

Шэрон Джонс оценила требования по защите библиотеки с информацией о клиентах, а также сведения о приложениях и отделах, которым потребуется доступ к этой информации. Она пришла к следующим выводам:

- Все отделы, за исключением склада и производственного отдела, должны иметь возможность изменения информации о клиентах.
- В профайлах всех сотрудников склада и производственного отдела установлен параметр Ограничение возможностей (Да), поэтому они имеют доступ только к ограниченному набору программ и меню. Эти меню позволяют просматривать информацию о клиентах, но не изменять ее.
- Для библиотеки записей о клиентах можно установить общие права доступа *CHANGE. Запрет на изменение записей определенными пользователями будет реализован с помощью меню. Однако в том случае, если в организации будут образованы новые отделы, то описанное разделение функций нужно будет проанализировать повторно.

Это пример упрощенной стратегии защиты. В данном случае ограничения реализованы с помощью пользовательских профайлов, а не с помощью ограничения прав доступа. Шэрон заполнила часть формы Описание библиотеки, относящуюся к общим правам доступа к библиотеке с информацией о клиентах (CUSTLIB).

Таблица 41. Пример формы Описание библиотеки компании JKL Toys—Часть 1: Информация о клиентах

Имя библиотеки: CUSTLIB	Описание: Информация о клиентах
Общие права доступа к библиотеке:	*USE
Общие права доступа к объектам библиотеки:	*CHANGE
Общие права доступа к новым объектам (CRTAUT):	*CHANGE

Шэрон Джонс определила, что некоторые временные файлы в библиотеке с информацией о клиентах удаляются в конце месяца приложением обработки дебиторской задолженности. Она решила управлять доступом к этим файлам отдельно, чтобы избежать случайного удаления других файлов из библиотеки. Для работы со всеми остальными объектами достаточно прав доступа *CHANGE.

Несмотря на то, что запуск очистки в конце месяца может выполняться несколькими лицами, Шэрон решила, что доступ к этим временным файлам не представляет собой никакой опасности. Она решила указать для этих файлов общие права доступа *ALL, а не ограничивать доступ, разрешая его только лицам, запускающим ежемесячную очистку. Ниже показана вторая часть формы Описание библиотеки для библиотеки с информацией о клиентах (CUSTLIB).

Таблица 42. Пример формы Описание библиотеки компании JKL Toys—Часть 2: Информация о клиентах

Список специальных прав доступа к объектам библиотеки				
Профайл пользователя или группы	Имя объекта	Тип объекта	Требуемые права доступа	Список прав доступа
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

Теперь вы можете принять решение о выборе общих прав доступа к библиотекам программ.

Определение общих прав доступа к библиотекам программ

Часто программы и файлы данных хранятся в разных библиотеках. Хотя это разделение и не обязательно, но многие программисты используют его при разработке приложений. Если объекты приложения распределены по нескольким библиотекам, необходимо выбрать общие права к этим библиотекам. Для запуска программы достаточно иметь права доступа *USE к этой программе и к ее библиотеке, но в

библиотеке программы часто находятся и другие объекты, необходимые для ее работы. Для определения оптимальных прав доступа к этим объектам задайте программисту следующие вопросы:

- Применяет ли приложение для взаимодействия между программами области данных или очереди сообщений? Находятся ли они в библиотеке программы? Для работы с этими объектами у приложения должны быть права доступа *CHANGE к ним.
- Удаляет ли приложение какие-либо объекты во время работы? Для удаления объекта необходимы права доступа *ALL к этому объекту.
- Создает ли приложение какие-либо объекты во время работы? Для создания новых объектов в библиотеке необходимы права доступа *CHANGE к библиотеке.

Занесите собранную информацию в обе части формы Описание библиотеки, оставив пустыми только поля Владелец библиотеки и Список прав доступа. См. раздел определение владельцев библиотек и объектов.

Просмотрите примеры прав доступа, выбранных Шэрон Джонс. В первом примере Шэрон решила, что для библиотеки программы Заказы клиентов оптимален упрощенный вариант защиты. Во втором примере для библиотеки программы Дебиторская задолженность выбран более строгий режим защиты.

Пример: Форма Описание библиотеки компании JKL Toys—Стратегия без ограничений: Шэрон Джонс исследовала библиотеку программы клиентских заказов и сделала следующие выводы:

- Для связи между программами применяется одна очередь сообщений COMSGQ01.
- Очередь сообщений периодически очищается, но никогда не удаляется. Для работы с очередью сообщений достаточно прав доступа *CHANGE.

Шэрон решила установить права доступа *USE для всех объектов библиотеки программ и отдельно определить очередь COMSGQ01. В приведенных ниже таблицах показана созданная Шэрон форма Описание библиотеки для библиотеки COPGMLIB:

Таблица 43. Пример формы Описание библиотеки компании JKL Toys: Библиотека программ

Описание библиотеки	**Часть 1 из 2**
Имя библиотеки: COPGMLIB	Описание: Библиотека программы клиентских заказов
Общие права доступа к библиотеке: *USE Общие права доступа к объектам библиотеки: *USE Общие права доступа к новым объектам (CRTAUT): *USE Владелец библиотеки:	

Таблица 44. Пример формы Описание библиотеки компании JKL Toys: Библиотека программ

Описание библиотеки				**Часть 2 из 2**
Список прав доступа к отдельным объектам библиотеки				
Профайл пользователя или группы	Имя объекта	Тип объекта	Требуемые права доступа	Списки прав доступа
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

Применение прав доступа для управления доступом к программе

Хотя большинство сотрудников JKL Toys могут изменять информацию о клиентах, устанавливать пределы кредитования разрешено лишь нескольким сотрудникам. Пределы кредитования задаются в основном файле клиентов (CUSTMAS), но изменяются специализированной программой ARPGM12 из библиотеки

ARPGMLIB. Шэрон может ограничить использование этой программы и предотвратить несанкционированное изменение пределов кредитования. В следующих таблицах показана заполненная форма описания библиотеки ARPGMLIB:

Таблица 45. Пример формы Описание библиотеки компании JKL Toys: Индивидуальные права доступа

Описание библиотеки	**Часть 1 из 2**
Имя библиотеки: ARPGMLIB	Описание: Библиотека программы дебиторской задолженности
Общие права доступа к библиотеке: *USE Общие права доступа к объектам библиотеки: *USE Общие права доступа к новым объектам (CRTAUT): *USE Владелец библиотеки:	

Таблица 46. Пример формы Описание библиотеки компании JKL Toys: Индивидуальные права доступа

Описание библиотеки				**Часть 2 из 2**
Список прав доступа к отдельным объектам библиотеки				
Профайл пользователя или группы	Имя объекта	Тип объекта	Требуемые права доступа	Списки прав доступа
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

Вы можете просмотреть пример стратегии с ограничениями, в котором используются принятые права доступа; затем вы можете выбрать владельцев библиотек и объектов.

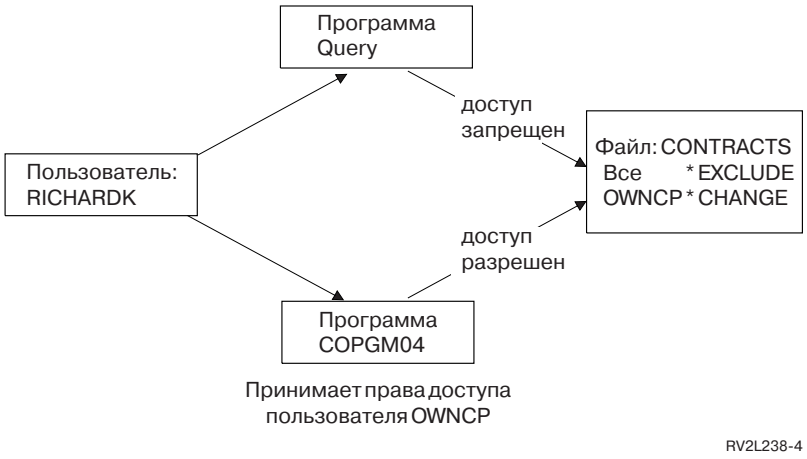
Пример: Форма Описание библиотеки компании JKL Toys—Стратегия с ограничениями: В предыдущих примерах продемонстрирован упрощенный поход к защите информации, при котором у большинства пользователей был доступ к данным библиотеки. Однако информация о контрактах и ценах компании JKL Toys считается конфиденциальной, поэтому доступ к ней следует ограничить. Вся эта информация хранится в отдельной библиотеке. Программы, применяемые для работы с этой информацией также находятся в отдельной библиотеке.

Шэрон оценила требования к защите приложения Контракты и цены (см. Определение защищаемых ресурсов). Кроме того, она просмотрела формы описания приложений и библиотек. По мнению Шэрон, адекватная защита данных при работе с этим приложением оказалась довольно сложной задачей. Поэтому она обсудила вопрос с поставщиком приложения и с учетом предъявляемых требований сделала следующие выводы:

- Сотрудники и менеджеры отдела продаж и маркетинга должны иметь возможность создания и изменения контрактов. Они могут работать как с файлами, так и с программами.
- Сотрудники отдела обработки заказов изменяют контракты и просматривают цены неявно при вводе заказов на поставку, однако просмотр контрактов и цен другим способом для них запрещен. При этом сотрудники будут использовать Query для создания отчетов о клиентах и заказах. Если предоставить им права доступа к файлам контрактов и цен, они смогут создавать программы на Query для их просмотра и печати.

Поставщик используемого в JKL Toys программного обеспечения предложил использовать для решения этой задачи функцию принятых прав доступа. Функция **принятых прав доступа** позволяет пользователю на время работы программы принять права доступа ее владельца. При этом пользователю не требуются права доступа к объекту.

На приведенной ниже схеме показан пример работы функции принятых прав доступа. У Карен Ричардс (RICHARDK) из отдела обработки заказов нет прав на использование файла контрактов. Тем не менее, во время ввода заказов, она должна просматривать и обновлять баланс по контрактам. Программа ввода заказов, работающая с балансами по контрактам (COPGM04), заимствует права доступа профайла OWNCP. Когда Карен работает с программой COPGM04, она получает права на использование файла контрактов.



Подробные сведения о принадлежности объектов приведены в разделе ″Определение принадлежности библиотек и объектов″. Разработчик или поставщик программы может настроить применение принятых прав доступа на этапе компиляции или с помощью команды Изменить программу (CHGPGM). Перед использованием этой функции необходимо точно определить все функции, которые выполняет программа.

Шэрон решила использовать функцию принятых прав доступа для предоставления доступа к файлу контрактов и цен сотрудникам, не работающим в отделе продаж и маркетинга. Она определила, что для работы приложения Контракты и цены достаточно предоставить права доступа *CHANGE к объектам. В приведенной ниже таблице показана форма описания библиотеки Контракты:

Таблица 47. Пример формы Описание библиотеки компании JKL Toys: Пример стратегии с ограничениями

Описание библиотеки		**Часть 1 из 2**
Имя библиотеки: CONTRACTS	Описание: Библиотека контрактов и цен	
Общие права доступа к библиотеке: *EXCLUDE Общие права доступа к объектам библиотеки: *CHANGE Общие права доступа к новым объектам (CRTAUT): *CHANGE Владелец библиотеки:		

Таблица 48. Пример формы Описание библиотеки компании JKL Toys: Пример стратегии с ограничениями

Описание библиотеки				**Часть 2 из 2**
Список прав доступа к отдельным объектам библиотеки				
Профайл пользователя или группы	Имя объекта	Тип объекта	Требуемые права доступа	Списки прав доступа

Таблица 48. Пример формы Описание библиотеки компании JKL Toys: Пример стратегии с ограничениями (продолжение)

DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

Запрещать доступ к объектам библиотеки не требуется, так как установлен запрет для всей библиотеки. Кроме этого, Шэрон предоставила права доступа менеджерам и сотрудникам отдела продаж и маркетинга. Для этого она использовала групповые права доступа, а не права, устанавливаемые для отдельных пользователей.

Примечание: Опытный программист, у которого был доступ к библиотеке, может сохранить возможность доступа к объектам даже после того, как его права доступа к библиотеке были аннулированы. Для обеспечения максимальной объекты библиотеки можно ограничить доступ не только к библиотеке, но и к ее объектам.

Вы можете просмотреть пример стратегии без ограничений, в котором используются общие права доступа; затем вы можете выбрать владельцев библиотек и объектов.

Определение принадлежности библиотек и объектов

После того как вы спланируете защиту библиотек приложений, вы можете задать принадлежность библиотек и объектов. Владелец объекта - это пользователь, который его создал. Владелец автоматически получает все права доступа к объекту, в частности, права на его изменение и удаление; кроме того, он может предоставлять другим пользователям права на использование данного объекта. Системный администратор может выполнять эти функции по отношению к любому объекту в системе.

В системе профайл владельца объекта применяется с целью отслеживать, кому предоставляются права доступа к объекту. Это внутренняя функция системы. Она не оказывает прямого влияния на профайл пользователя. Однако, если вы неправильно спланируете принадлежность объекта, некоторые профайлы пользователей могут стать очень большими.

При сохранении объекта система сохраняет вместе с ним и имя профайла его владельца. Система использует эту информацию при восстановлении объекта. Если в системе нет профайла владельца восстанавливаемого объекта, то информация о принадлежности объекта передается в поставляемый фирмой IBM профайл с именем QDFTOWN.

Рекомендации

Приведенные ниже рекомендации применимы во многих, но отнюдь не во всех случаях. После прочтения этих рекомендаций обсудите ваши идеи относительно принадлежности объектов с разработчиком или поставщиком программного приложения. Если вы приобрели готовые приложения, то не исключено, что вы не сможете установить, какому профайлу принадлежат библиотеки и объекты. Приложение может быть спроектировано таким образом, что изменение принадлежности объектов будет запрещено.

- Не назначайте поставляемые фирмой IBM профайлы (такие как QSECOFR или QPGMR) в качестве владельцев приложений. Этим профайлам и так принадлежит большое число объектов в поставляемых фирмой IBM библиотеках, и размер их достаточно велик.
- Профайл группы обычно не следует делать владельцем приложения. Все члены группы по умолчанию обладают такими же правами доступа, что и профайл группы, если только вы не аннулировали часть прав доступа у некоторых членов группы. Сделав профайл группы владельцем приложения, вы тем самым предоставляете полные права доступа к приложению каждому члену группы.
- Если вы планируете передать полномочия по управлению приложениями администраторам из других отделов, то вы можете назначить администраторов владельцами всех объектов в этих приложениях. Однако помните, что круг обязанностей администратора приложения может измениться. В этом случае вам придется передать полномочия другому администратору.

- Широко распространен прием, который заключается в создании для каждого приложения специального профайла владельца с паролем *NONE. Профайл владельца используется системой для управления предоставлением прав доступа к данному приложению. Фактически приложением управляет системный администратор (или пользователь с соответствующими правами доступа), который, однако, может передать свои полномочия администраторам с правами доступа *ALL к определенным приложениям.

Решите, каким профайлам должны принадлежать ваши приложения. Введите информацию о профайле владельца в каждую форму Описание библиотеки.

Перед тем как устанавливать принадлежность пользовательских библиотек и права доступа к ним, полезно ознакомиться с примером, в котором показано, как определяется принадлежность приложения в компании JKL Toys.

Пример: Форма Описание принадлежности приложений компании JKL Toy

Шэрон Джонс решила создать профайл владельца для каждого приложения. Шэрон и Кен Гаррисон, ответственный за резервное копирование, будут управлять защитой приложений. В дальнейшем, если система защиты компании усложнится, Шэрон можете делегировать ряд функций по управлению правами доступа менеджерам отделов.

Шэрон добавила новую запись в форму Соглашения о присвоении имен:

Таблица 49. Форма Соглашение о присвоении имен в JKL Toy Company: Пример профайла владельца

Тип объекта	Соглашение о присвоении имен
Профайл владельца	Профайл владельца должен быть создан для каждого приложения. Ему будут принадлежать все библиотеки приложения и находящиеся в них объекты. Имя профайла будет состоять из префикса OWN и краткого названия приложения. Например, приложению Управление запасами (Inventory Control) будет соответствовать профайл владельца OWNIC.

Шэрон решила, что названия всех профайлов владельцев должны начинаться с символов OWN, чтобы в меню и списках эти профайлы были показаны рядом.

Шэрон выбрала владельцев для всех библиотек приложений и зафиксировала этот выбор в форме Соглашения о присвоении имен. Единственной библиотекой, для которой нашлось несколько потенциальных претендентов на роль владельца, оказалась библиотека с информацией о клиентах. В связи с тем, что для создания новых записей о клиентах и установки пределов кредитования используется приложение Дебиторская задолженность, Шэрон решила, что файлы с записями о клиентах должны принадлежать ему. Были назначены следующие владельцы:

Имя библиотеки	Имя владельца
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

Следующим этапом является настройка принадлежности и прав доступа для пользовательских библиотек.

Определение принадлежности пользовательских библиотек и предоставление доступа к ним

Если в вашей системе установлена лицензионная программа IBM Query для iSeries или другая программа поддержки принятия решений, то вашим пользователям потребуется библиотека для хранения создаваемых

ими запросов. Обычно с этой целью применяется **текущая библиотека** пользовательского профайла. Дополнительная информация о создании текущей библиотеки для каждого пользователя приведена в разделе "Выбор значений, управляющих входом в систему". Например, Шэрон Джонс планирует использовать для отдела сбыта текущие библиотеки, а для других отделов - библиотеки групп:

- Сотрудники отдела сбыта будут интенсивно работать с программой Query. У каждого пользователя должна быть частная библиотека. В противном случае возможны недоразумения при присвоении имен запросам и случайное удаление пользовательских программ.
- Другим отделам для начала будут выделены библиотеки групп. Если они будут создавать много программ Query, можно рассмотреть вопрос о создании частных библиотек.

Если пользователь входит в состав группы, то в специальном поле в профайле пользователя указывается, кому принадлежат созданные им объекты: пользователю или его группе. Если объекты принадлежат пользователю, то вы можете указать, какие права предоставляются членам группы по отношению к этим объектам. Вы можете также определить тип прав доступа для группы: основные права доступа группы или частные права доступа. Первый вариант предпочтительнее в плане производительности системы. Шэрон делает дополнительные замечания о библиотеках пользователей:

- Создаваемые объекты должны принадлежать сотрудникам отдела сбыта, а не группе. Сотрудникам этого отдела не требуется изменять программы запросов других сотрудников.
- Любой пользователь группы должен иметь возможность запускать программы Query других пользователей группы, т.е. группа получает права доступа *USE к любому объекту, создаваемому пользователем группы.
- Права доступа группы - это основные права доступа.
- Пользователям с общими правами доступа запрещено обращаться к этим библиотекам. Сотрудники отдела сбыта могут создавать файлы вывода на основе своих запросов. Эти файлы могут содержать конфиденциальную информацию.
- Группа, включающая сотрудников любого другого отдела, будет владеть библиотекой группы и всеми создаваемыми в ней объектами. Все члены группы могут изменять или удалять любой объект из этой библиотеки. Если это вызовет проблемы, можно попробовать другой способ.

Ниже приведена таблица с формой Профайл пользователя для отдела сбыта, в котором объекты принадлежат пользователю:

Таблица 50. Форма Профайл пользователя компании JKL Toys: пример объектов, принадлежащих пользователю

Имена профайлов группы: DPTSM	
Владелец создаваемых объектов: *USRPRF	Права доступа группы к создаваемым объектам: *USE
Тип прав доступа группы: *PGP	

Ниже приведена таблица с формой Профайл пользователя для отдела, в котором объекты принадлежат группе:

Таблица 51. Форма Профайл пользователя компании JKL Toys: пример объектов, принадлежащих группе

Имена профайлов группы: DPTxx	
Владелец создаваемых объектов: *GRPPRF	Права доступа группы к создаваемым объектам:

Если владелец создаваемых объектов - группа, то поле **Права доступа группы к создаваемым объектам** не используется. Члены группы автоматически получают права доступа *ALL ко всем создаваемым объектам.

Решите, кто должен быть владельцем библиотек пользователей и кому следует предоставлять доступ к ним. Укажите эти параметры в поле **Владелец создаваемых объектов** и **Права доступа группы к объектам** в форме Профайл пользователя. Теперь вы готовы к объединению объектов в группы.

Создание групп объектов

После того как вы задали принадлежность библиотек и объектов, вы можете начать объединение объектов в группы. Для того чтобы упростить управление правами доступа, воспользуйтесь списком прав доступа и объедините объекты с одинаковыми правами доступа в одну группу. Тогда вы сможете создавать общие профайлы, профайлы группы и пользовательские профайлы не для каждого отдельного пользователя, а для списка прав доступа. Система считает объекты, защищаемые списком прав доступа, одинаковыми, однако вы можете предоставлять разным пользователям разные права доступа ко всему списку.

Список прав доступа упрощает переопределение прав доступа при восстановлении объектов. Если вы защищаете объекты с помощью списка прав доступа, то при восстановлении объекты будут автоматически связываться со списком.

Вы можете предоставить пользователю или группе права на управление списком прав доступа (*AUTLMGT). При этом пользователь сможет добавлять других пользователей в список или удалять их из списка, а также изменять права доступа, предоставленные другим пользователям.

Рекомендации

- Создавайте списки прав доступа для объектов, которые необходимо защитить, причем более-менее одинаково. При использовании списков прав доступа вы имеете дело не с отдельными правами доступа, а с их категориями. Кроме того, списки прав доступа облегчают восстановление объектов и контроль за предоставлением прав доступа в вашей системе.
- Избегайте сложных схем, в которых объединены списки прав доступа, права доступа группы и права доступа отдельного пользователя. Выберите один способ, который лучше всего отражает требования защиты, вместо того чтобы применять все способы одновременно.

Описание соглашения о присвоении имен для списков прав доступа необходимо добавить в форму Соглашения о присвоении имен.

После того как вы составите форму Список прав доступа, вернитесь к форме Описание библиотеки и добавьте в нее необходимую информацию. Возможно, что списки прав доступа уже созданы программистом или поставщиком пакета прикладных программ. Не забудьте свериться с ними.

Прежде чем приступить к планированию защиты для принтеров и вывода на принтер, ознакомьтесь с примером, в котором показано, как Шэрон Джонс из компании JKL Toys планирует списки прав доступа.

Пример: Форма Список прав доступа компании JKL Toys

Шэрон просмотрела описание библиотеки с информацией о клиентах и решила создать список прав доступа для файлов, которые очищаются в конце каждого месяца. Несмотря на то, что очищается только три файла, для упрощения работы Шэрон решила использовать списки прав доступа. Если в дальнейшем потребуется выполнять очистку дополнительных файлов, Шэрон сможет легко изменить процедуру. Шэрон решила запретить доступ обычных пользователей к этим файлам, чтобы избежать возможных ошибок. Она предоставила права пользователя *ALL только тем пользователям, которые запускают ежемесячную обработку. Роуз Виллис - системный оператор второй смены - ей также может понадобиться информация об этих файлах. В связи с этим ей необходимо предоставить права доступа *USE.

В следующей таблице показаны соглашения о присвоении имен, которое Шэрон использовала при составлении списка прав доступа:

Таблица 52. Форма Соглашение о присвоении имен в JKL Toy Company: Пример списка прав доступа

Форма Соглашение о присвоении имен		
Составлено: Шэрон Джонс		Дата: 9/5/99
Тип объекта	**Соглашение о присвоении имен**	

Таблица 52. Форма Соглашение о присвоении имен в JKL Toy Company: Пример списка прав доступа (продолжение)

Списки прав доступа	Имена списков, используемых для защиты объектов из одной библиотеки, состоят из части имени библиотеки, символов LST и номера. Например, для объектов из библиотеки CUSTLIB будет применяться список с именем CUSTLST1. При защите объектов из нескольких библиотек в имени списка рекомендуется использовать имя приложения, например ARLST1. Если список относится к нескольким приложениям, присвойте ему понятное имя. В описании списка должно быть указано его основное назначение.

В приведенной ниже таблице показана форма Список прав доступа для библиотеки CUSTLIB. Шэрон составила эту форму на основе информации из формы Описание библиотеки:

Таблица 53. Пример: Форма План списка прав доступа компании JKL Toys

Форма Список прав доступа					
Имя списка прав доступа: CUSTLST1					
Описание: Файлы, очищаемые в конце месяца.					
Список объектов, защищаемых этим списком					
Имя объекта	Тип объекта	Библиотека объекта	Имя объекта	Тип объекта	Библиотека объекта
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
Список групп и пользователей, имеющих доступ к этому списку					
Группа или пользователь	Разрешенный тип доступа	Разрешить управление списком	Группа или пользователь	Разрешенный тип доступа	Разрешить управление списком
PUBLIC	*EXCLUDE	нет	ROSSG	*ALL	нет
SMITHJ	*ALL	нет	JONESS	*ALL	да
WILLISR	*USE	нет			

Шэрон также добавила сведения о списках прав доступа в форму Описание библиотеки CUSTLIB:

Форма Описание библиотеки				Часть 2 из 2
Составлено: Шэрон Джонс			Дата: 9/9/99	
Имя библиотеки: CUSTLIB				
Список специальных прав доступа к объектам библиотеки				
Профайл пользователя или группы	Имя объекта	Тип объекта	Требуемые права доступа	Список прав доступа
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

Для того чтобы система использовала список прав доступа при определении общих прав доступа к объекту, необходимо в параметре общих прав доступа указать значение *AUTL.

Просмотрите права доступа пользователей и групп, указанные в форме Описание библиотеки. Определите, насколько оправдано применение списков прав доступа. Если вы решите их использовать, подготовьте

форму Список прав доступа и добавьте информацию о списках прав доступа в формы Описание библиотеки. После этого вы можете перейти к планированию защиты принтеров и вывода.

Планирование защиты принтеров и вывода на принтер

После того как вы сгруппировали объекты, необходимо спланировать защиту вывода на принтер. Вы уже планировали систему защиты информации, хранящейся в вашей системе. Теперь нужно запланировать защиту конфиденциальной информации, которая печатается или ожидает печати. Принтеры, используемые в вашей фирме для печати конфиденциальной информации, указаны в Плане физической защиты.

Когда вы запускаете программу, которая печатает отчет, то он, как правило, поступает на принтер не сразу. Сначала программа создает копию отчета, называемую **буферным файлом** или **выводом на принтер**. Пока принтер недоступен, система хранит буферный файл в объекте, называемом **очередь вывода**. Пока буферный файл находится в очереди вывода, вы можете просматривать этот отчет на своей рабочей станции. Вы также можете приостановить его отправку на принтер или направить его на конкретный принтер.

Буферизация упрощает планирование заданий принтера и работу с общими принтерами, а также установку защиты конфиденциальной информации при ее выводе на принтер. Можно создать одну или несколько специальных очередей для вывода конфиденциальной информации и ограничить доступ к этим очередям. Кроме того, вы можете отслеживать, когда конфиденциальная информация передается из очереди вывода на принтер.

При чтении данного раздела постепенно заполняйте форму Защита рабочей станции и вывода на принтер.

При создании специальной очереди вывода можно задать несколько параметров, связанных с защитой:

- **Параметр Показывать данные (DSPDTA)**: Параметр DSPDTA очереди вывода определяет, может ли пользователь просматривать, отправлять или копировать буферный файл, принадлежащий другому пользователю.
- **Параметр Права на исправление (AUTCHK)**: Параметр AUTCHK очереди вывода определяет, может ли пользователь изменять или удалять буферный файл, принадлежащий другому пользователю.
- **Параметр Управляется оператором (OPRCTL)**: Параметр OPRCTL очереди вывода определяет, разрешено ли пользователю с правами доступа *JOBCTL (или с классом *SYSOPR) управлять очередью вывода.

Параметры очереди вывода и предоставленные пользователю права доступа к очереди вывода и специальные права доступа совместно определяют, какие функции над буферными файлами в очереди вывода может выполнять данный пользователь. В приведенной ниже таблице перечислены комбинации этих параметров, позволяющие выполнять различные функции.

Функции печати	Параметр очереди вывода			Права доступа к очереди вывода	Специальные права доступа
	DSPDTA	AUTCHK	OPRCTL		
Добавление буферного файла в очередь[1]	Любые	Любые	Любые	*READ	Нет
	Любые	Любые	*YES	Любые	*JOBCTL
Просмотр списка буферных файлов (команда WRKOUTQ)[2]	Любые	Любые	Любые	*READ	Нет
	Любые	Любые	*YES	Любые	*JOBCTL
Просмотр, копирование и пересылка буферных файлов (DSPSPLF, CPYSPFL, SNDNETSPLF, SNTCPSPLF)[2]	*YES	Любые	Любые	*READ	Нет
	*NO	*DTAAUT	Любые	*CHANGE	Нет
	*NO	*OWNER	Любые	Владелец[3]	Нет
	*YES	Любые	*YES	Любые	*JOBCTL
	*NO	Любые	*YES	Любые	*JOBCTL
	*OWNER[5]	Любые	Любые	Любые	Любые

Изменение, удаление, блокирование, разблокирование буферного файла (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF)[2]	Любые	*DTAAUT	Любые	*CHANGE	Нет
	Любые	*OWNER	Любые	Владелец[3]	Нет
Изменение, очистка, блокирование и разблокирование очереди вывода (CHGOUTQ, CLROUTO, HLDOUTQ, RLSOUT)[2]	Любые	*DTAAUT	Любые	*CHANGE	Нет
	Любые	*OWNER	Любые	Владелец[3]	Нет
	Любые	Любые	*YES	Любые	*JOBCTL
Запуск загрузчика для очереди (STRPRTWTR, STRRMTWTR)[2]	Любые	*DTAAUT	Любые	*CHANGE[4]	Нет
	Любые	Любые	*YES	Любые[4]	*JOBCTL

1 Эти права доступа необходимы для отправки вывода в очередь вывода.

2 Вводите эти команды или используйте эквивалентные им опции меню.

3 Вы должны быть владельцем очереди вывода.

4 Кроме этого, необходимы права доступа *USE к описанию принтера.

5 Вы должны быть владельцем буферного файла или обладать специальными правами доступа *SPLCTL.

Просмотрите раздел Плана физической защиты, относящийся к принтеру. Используя приведенную выше информацию, заполните раздел формы Защита рабочей станции и вывода на принтер, относящийся к очереди вывода.

Перед тем как планировать защиту ресурсов для рабочих станций, рекомендуется ознакомиться с примером, в котором показано, как Шэрон Джонс из компании JKL Toys определяет значения этих параметров для очереди вывода.

Пример: Форма Защита очередей вывода и рабочих станций компании JKL Toys—Раздел очередей вывода

Отдел продаж и маркетинга компании JKL Toys предъявляет следующие требования по защите печати:

- При планировании изменения цен печатаются предварительные варианты прейскурантов. Эта информация должна быть недоступной для всех лиц за пределами отдела продаж и маркетинга, за исключением менеджеров компании.
- Информация о контрактах на время переговоров является конфиденциальной. Приблизительный начальный план контракта должен быть доступен только сотруднику, проводящему переговоры, и недоступен всем остальным сотрудникам отдела продаж и маркетинга.

Шэрон приняла решение о создание двух специализированных очередей вывода:

PRICEQ

Очередь вывода для печати предварительных вариантов прейскурантов. Эта очередь доступна всем сотрудникам отдела продаж и маркетинга. Очередь недоступна для сотрудников других отделов, включая системных операторов. Очередь PRICEQ находится в библиотеке CONTRACTS.

NEWCP

Очередь вывода для печати контрактов, находящихся на этапе согласования. Очередь предназначена для общего использования пользователями из отдела продаж маркетинга, но управлять буферными файлами могут только их владельцы. Очередь NEWCP находится в библиотеке CONTRACTS.

Ниже приведена часть формы Защита очередей вывода и рабочих станций, заполненная Шэрон для этих очередей:

Таблица 54. Пример формы Защита очередей вывода и рабочих станций компании JKL Toys: очередь вывода

Список параметров защищенных очередей вывода:

Таблица 54. Пример формы Защита очередей вывода и рабочих станций компании JKL Toys: очередь вывода (продолжение)

Имя очереди вывода	Библиотека очереди вывода	Показывать любые файлы (DSPDTA)	Права доступа для проверки (AUTCHK)	Управляется оператором (OPRCTL)
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

В разделе Определение общих прав доступа к библиотекам программ приведен пример настройки прав доступа для библиотеки CONTRACTS компании JKL Toys. Доступ к библиотеке разрешен только менеджерам из отдела продаж и маркетинга. В качестве общих прав доступа к библиотеке (включая очереди вывода) установлено значение *CHANGE.

В связи с тем, что параметр AUTCHK очереди вывода NEWCP имеет значение *OWNER, работать с буферным файлом может только его владелец (см. приведенную выше таблицу Права, необходимые для выполнения функций печати). Таким образом, сотрудники отдела продаж и маркетинга не могут печатать чужие контракты и просматривать файлы контрактов, находящиеся в очереди вывода.

После завершения планирования защиты очередей вывода вы можете перейти к планированию защиты рабочих станций.

Планирование защиты для рабочих станций

После планирования защиты принтеров и вывода на принтер можно приступить к планированию защиты для рабочей станции. В Плане по физической защите вы должны были перечислить рабочие станции, наиболее ненадежные с точки зрения защиты (в силу их расположения). На основе этой информации решите, к каким рабочим станциям следует ограничивать доступ.

Проинформируйте сотрудников, использующих эти рабочие станции, о необходимости соблюдать требования защиты. Покидая свое рабочее место, сотрудник обязательно должен выходить из системы. Рекомендуем вам письменно оформить требования к процедурам выхода из системы для уязвимых с точки зрения безопасности рабочих станций. Для того чтобы свести риск нарушения защиты к минимуму, вы можете также ограничить набор функций, которые разрешается выполнять на данной рабочей станции.

Простейший способ сделать это - разрешить доступ к рабочей станции только пользовательским профайлам с ограниченным набором функций. Именно такой способ применяет Шэрон Джонс для складского отдела компании JKL Toys. Она разрешает работникам грузового терминала Рэю Вагнеру и Дженис Эймс запускать только программу получения списка товаров на складе. Кроме того, только этим двум сотрудникам разрешено входить в систему с рабочей станции, установленной на складе.

Вы можете ограничить число рабочих станций, с которых системные администраторы могут входить в систему. Если задать системное значение QLMTSECOFR, то сотрудники с правами доступа системного администратора смогут входить в систему только со специально предназначенных для этого рабочих станций.

Подготовьте часть формы Защита очереди вывода и рабочей станции, относящуюся к рабочей станции.

При выполнении этой задачи вам поможет пример, в котором показано, как Шэрон Джонс заполнила эту форму. Просмотрите, кроме того, список рекомендаций по защите ресурсов, чтобы удостовериться, что ваш план защиты ресурсов достаточно прост и полон. После того как вы ознакомитесь с примером и рекомендациями, вы можете приступить к планированию установки приложений.

Пример: Форма Защита очередей вывода и рабочих станций компании JKL Toys—Раздел рабочих станций

Шэрон Джонс просмотрела план физической защиты и определила, какие рабочие станции могут представлять потенциальную угрозу для безопасности системы. Например, к рабочим станциям,

расположенным на складе и в удаленном торговом офисе, легко могут получить доступ посторонние лица. В плане физической защиты Шэрон отметила, что эти рабочие станции представляют потенциальную опасность.

Простейшим способом защиты таких рабочих станций является применение пользовательских профайлов с ограниченными возможностями. Шэрон использовала этот метод защиты в складском отделе компании JKL Toys. Шэрон разрешила Рэю Вагнеру и Дженис Эмис, работающим на приеме товаров, запускать только программу приема товаров. Кроме этого, она запретила всем остальным пользователям вход в систему с этих рабочих станций.

Шэрон повторно оценила требуемую настройку системного значения QLMTSECOFR. Для обеспечения дополнительной защиты рабочих станций, находящихся на складе и в удаленном торговом офисе, она решила установить значение 1 (Да).

Ниже приведена часть формы Защита очередей вывода и рабочих станций, заполненная Шэрон для этих рабочих станций:

Таблица 55. Пример формы Защита очередей вывода и рабочих станций компании JKL Toys: рабочие станции

Рабочие станции системного администратора: Если администратор может использовать только ограниченный набор рабочих станций (системное значение QLMTSECOFR = yes), то перечислите рабочие станции, которые должны быть доступны для системного администратора и пользователей с правами доступа *ALLOBJ: `Все рабочие станции, кроме перечисленных ниже.`	
Перечислите права доступа для рабочих станций с ограничениями:	
Имя рабочей станции	Группы или пользователи, имеющие доступ (права доступа *CHANGE)
`DSP10`	`AMESJ, WAGNERR`
`DSP11`	`AMESJ, WAGNERR`
`RMT01`	`UNGERJ, BELLB`
`RMT02`	`UNGERJ, BELLB`

Теперь вы можете ознакомиться с обзором рекомендаций по защите ресурсов или перейти к планированию установки приложений.

Общие рекомендации по защите ресурсов

После завершения планирования защиты для рабочей станции вы можете ознакомиться с приведенными ниже рекомендациями по защите ресурсов. В iSeries существует множество вариантов защиты информации. Тем самым вам предоставляется возможность гибкого планирования системы защиты ресурсов, наиболее полно отвечающей потребностям вашей компании. Однако такое многообразие возможностей может и сбить вас с толку.

На примере компании JKL Toy в данном разделе демонстрируется подход к планированию защиты ресурсов, основанный на следующих принципах:

- Переходите от общего к частному:
  - Выполните планирование для библиотек. Планирование для отдельных объектов выполняйте только в случае необходимости.
  - Сначала выполняйте планирование общих прав доступа, затем - прав доступа группы и только потом - индивидуальных прав доступа.
- Для повышения производительности и упрощения процедуры резервного копирования и восстановления данных задавайте специальные права доступа только к таким объектам, для защиты которых недостаточно общих прав доступа.
- Для новых объектов в библиотеке (значение CRTAUT) задавайте те же общие права доступа, что вы определили для большинства существующих объектов в этой библиотеке.

- Постарайтесь не предоставлять группам или отдельным пользователям меньше прав доступа, чем это предусматривают общие права. Это может привести к снижению производительности и к ошибкам, а также затрудняет контроль за действиями в системе. Если вы знаете, что все пользователи обладают как минимум общими правами доступа к объекту, вам легче планировать защиту и контролировать действия в системе.
- Для объединения в группы объектов с одинаковыми требованиями к защите используйте списки прав доступа. Управлять списками прав доступа гораздо легче, чем правами доступа отдельного пользователя, кроме того, они упрощают восстановление информации о защите.
- В качестве владельцев приложений создавайте специальные профайлы пользователей. Устанавливайте пароль владельца *NONE.
- Не задавайте в качестве владельцев приложений профайлы, поставляемые фирмой IBM (такие как QSECOFR или QPGMR).
- Для печати конфиденциальных отчетов применяйте специальные очереди вывода. Размещайте очередь вывода в той же библиотеке, в которой находится конфиденциальная информация.
- Ограничьте число сотрудников с правами доступа системного администратора.
- Будьте осторожны, предоставляя права доступа *ALL к объектам или библиотекам. Пользователям с правами доступа *ALL разрешено удалять объекты.

Если вы успешно спланировали защиту ресурсов, вам не составит труда выполнить следующие действия:
- Для каждой библиотеки приложений заполните Части 1 и 2 формы Описание библиотеки.
- В формах Профайл пользователя заполните поля **Владелец создаваемых объектов** и **Права доступа группы к создаваемым объектам**.
- В форме Соглашения о присвоении имен опишите свой способ присвоения имен спискам прав доступа.
- Подготовьте формы Список прав доступа.
- Добавьте информацию о списках прав доступа в формы Описание библиотеки.
- Подготовьте форму Защита очереди вывода и рабочей станции.

Теперь вы готовы к тому, чтобы начать планирование установки приложений.

Планирование установки приложений

Для того чтобы завершить планирование защиты ресурсов, вам необходимо подготовиться к установке приложений. Информация в приведенных ниже разделах поможет вам спланировать принадлежность приложений и права доступа к ним после их установки. Описанные здесь способы применимы не ко всем приложениям. Для разработки оптимального плана установки проконсультируйтесь с программистом или с разработчиком приложения.

Если вы будете устанавливать приложение, полученное от разработчика, то следующая информация поможет вам спланировать действия по защите, которые вам необходимо выполнять до и после загрузки библиотек приложения.

Если вы будете устанавливать приложение, разработанное вашим программистом, то следующая информация поможет вам спланировать действия по защите, необходимые для перевода приложения из состояния тестирования в рабочее состояние.

Выполните описанную ниже процедуру для одного приложения. Затем вернитесь к ее началу и подготовьте формы Установка приложения для остальных приложений.

Какие формы вам потребуются?

Сделайте копии перечисленных ниже форм и заполните их в соответствии с информацией раздела:

Таблица 56. Подготовка форм, необходимых для планирования установки приложений

Название формы	**Необходимое число копий**
Форма Установка приложения	По одной на каждое приложение

Для сбора информации, необходимой для планирования установки приложений, воспользуйтесь формами, с которыми вы уже работали:

Название формы	**Подготовлена в разделе:**
Форма Описание библиотеки	Создание описаний библиотек
Форма Список прав доступа	Создание групп объектов

Процедура установки приложений приведена в разделе Загрузка приложений.

Информация о планировании установки приложений приведена в следующих разделах:

- Определение профайлов пользователей и параметров установки для приложений.
- Изменение параметров установки.

Определение профайлов пользователей и параметров установки для приложений

При планировании установки приложений вам прежде всего необходимо выбрать для каждого приложения профайлы пользователей и параметры установки. Перед установкой приложений, созданных в других системах, необходимо создать один или несколько пользовательских профайлов. Для загрузки библиотек приложения в системе должен существовать профайл пользователя - владелец библиотек и объектов этого приложения. В форме Установка приложения укажите, какие профайлы и с какими параметрами потребуются вам для создания каждой библиотеки.

Для определения нужных параметров установки задайте своему программисту или поставщику приложений следующие вопросы, а ответы запишите в форме Установка приложения:

- Какой профайл владеет библиотекой приложения?
- Какой профайл владеет объектами в этой библиотеке?
- Каковы общие права доступа к этой библиотеке (AUT)?
- Каковы общие права доступа к новым объектам (CRTAUT)?
- Каковы общие права доступа к объектам в этой библиотеке?
- Какие программы (если они есть) принимают права доступа владельца?

Проверьте, нет ли для данного приложения списка прав доступа, созданного программистом или поставщиком. Для каждого такого списка подготовьте форму Список прав доступа или обратитесь к своему программисту за информацией об этом списке.

Вы можете определить, нужно ли изменять какие-либо параметры установки.

Изменение параметров установки приложений

Сравните информацию, указанную в форме Установка приложения, с планом защиты ресурсов для библиотеки (форма Описание библиотеки). Если они различны, вам нужно решить, какие изменения необходимо сделать после установки приложения.

Изменение принадлежности приложения

Если ваш программист или поставщик приложения создали специальный профайл, которому принадлежат библиотеки и объекты приложения, рекомендуем вам использовать именно его, даже если его имя не соответствует применяемому соглашению. Передача принадлежности объектов занимает длительное время, поэтому ее следует избегать.

Если приложение принадлежит одному из профайлов группы, поставляемых фирмой IBM (например, QSECOFR или QPGMR), то после установки приложения необходимо передать права на владение им другому профайлу.

Некоторые программисты устанавливают запрет на изменение принадлежности объектов в создаваемых ими приложениях. Постарайтесь соблюдать эти ограничения, но не в ущерб своим собственным требованиям к защите системы. Однако, если приложение принадлежит профайлу, поставляемому фирмой IBM (например, QSECOFR), то вам вместе с программистом или поставщиком приложения необходимо продумать план по изменению принадлежности. В идеальном случае вы должны изменить принадлежность приложения до того, как оно будет установлено.

Изменение общих прав доступа

При сохранении объектов вместе с ними сохраняются и права доступа к ним. Если вы восстанавливаете библиотеку приложения в системе, то права доступа к этой библиотеке и к ее объектам будут такими же, как в момент сохранения. Это верно и для библиотек, сохраненных в других системах.

Значение CRTAUT, указанное для библиотеки (общие права доступа к новым объектам), не влияет на права доступа к восстанавливаемым объектам. Независимо от значения CRTAUT для библиотеки, объекты восстанавливаются с теми же общими правами доступа, которые существовали в момент сохранения.

Вы должны изменить общие права доступа к библиотекам и объектам в соответствии с планом, заданным в форме Описание библиотеки.

При планировании установки приложений рекомендуем ознакомиться с примером такого планирования в компании JKL Toys.

Для того чтобы гарантировать, что вы запланировали установку всех необходимых приложений, выполните следующие действия:

- Завершите заполнение первой формы Установка приложения. Затем вернитесь к началу процедуры и подготовьте формы для остальных приложений.
- Проверьте все формы и убедитесь, что они заполнены полностью. Сделайте копии этих форм и храните их в надежном месте, пока не установите систему и лицензионные программы.

После того как вы выполните эти задачи планирования, вы сможете перейти к настройке защиты для пользователей.

Пример: Форма Установка приложений в компании JKL Toy: Компания JKL Toys приобрела приложения Заказы клиентов и Дебиторская задолженность у компании-поставщика приложений. Кроме этого, компания наняла программиста для разработки приложения Контракты и цены и его интеграции с приложением Заказы клиентов.

Шэрон Джонс заполнила формы Установка приложений, используя информацию из форм описания библиотек. В следующей таблице показана форма Описание библиотеки CUSTLIB: (см. раздел ″Описание библиотеки.″)

Таблица 57. Пример формы Описание библиотеки компании JKL Toys

Описание библиотеки	**Часть 1 из 2**
Составлено: Шэрон Джонс	Дата: 9/9/99
Имя библиотеки: CUSTLIB	Описание: Библиотека с информацией о клиентах

Таблица 57. Пример формы Описание библиотеки компании JKL Toys (продолжение)

Кратко опишите назначение библиотеки: Библиотека содержит все сведения о клиентах, включая файлы заказов и счетов.
Определите требования по защите библиотеки, например, уровень конфиденциальности хранящейся в ней информации: На данный момент просмотр заказов разрешен всем сотрудникам компании. Для сохранения целостности информации необходимо ограничить возможность ее изменения.
Общие права доступа к библиотеке: *USE Общие права доступа к объектам библиотеки: *CHANGE Общие права доступа к новым объектам (CRTAUT): *CHANGE Владелец библиотеки: OWNAR

В приведенной ниже таблице показана форма Установка приложений, заполненная Шэрон для приложения Заказы клиентов. Обратите внимание, что Шэрон решила использовать профайл владельца, созданный поставщиком приложения. Профайлу COWNER будут принадлежать как библиотеки файлов, так и библиотеки программ.

После установки приложения Шэрон должна выполнить следующие действия:

- Изменить общие права доступа к библиотекам в соответствии с планом защиты ресурсов, зафиксированным в формах Описание библиотеки.
- Изменить класс профайла COWNER на *USER и аннулировать специальные права доступа.
- Изменить пароль профайла COWNER на *NONE.

Таблица 58. Пример формы Установка приложения в компании JKL Toys

Имя приложения: Заказы клиентов (CO)		Описание: Ввод, просмотр и обслуживание заказов.
Перечислите все профайлы, которые должны быть созданы при установке приложения, и объясните их назначение: Библиотека, содержащая файлы, принадлежит профайлу COWNER. Программная библиотека принадлежит профайлу QPGMR.		
Имя библиотеки: CUSTLIB		
	До установки	**После установки**
Владелец библиотеки	COWNER	COWNER
Владелец объекта	COWNER	COWNER
Общие права доступа к библиотеке	*EXCLUDE	*USE
Общие права доступа к объектам	*ALL	*CHANGE
Общие права доступа к новым объектам	*CHANGE	*CHANGE
Имя библиотеки: COPGMLIB		
	До установки	**После установки**
Владелец библиотеки	QPGMR	COWNER
Владелец объекта	QPGMR	COWNER
Общие права доступа к библиотеке	*EXCLUDE	*USE
Общие права доступа к объектам	*ALL	*CHANGE
Общие права доступа к новым объектам	*CHANGE	*CHANGE

По окончании планирования вы можете перейти к настройке защиты для пользователей.

Настройка защиты для пользователей

В данном разделе описаны задачи, выполняемые для настройки защиты в вашей системе с помощью интерфейса командной строки. Если вы настраиваете новую систему, выполните последовательно все перечисленные шаги. При переходе к следующему шагу система использует информацию, заданную на предыдущих шагах. Для настройки основной защиты системы необходимо выполнить два набора задач. Во-первых, нужно определить защиту для пользователей, во-вторых, защитить ресурсы в системе. Этапы настройки защиты для пользователей и ресурсов описаны, соответственно, в двух приведенных ниже таблицах.

Примечание: Сначала вы **ОБЯЗАНЫ** выполнить все этапы настройки защиты для пользователей. Только затем вы можете приступить к настройке защиты ресурсов.

Таблица 59. Этапы настройки защиты для пользователей

Этап	Ваши действия	Необходимые формы
Настройка общей среды	Задайте начальные системные значения и сетевые атрибуты. Создайте профайл администратора системы.	Форма Выбор системных значений
Настройка системных значений для защиты	Задайте дополнительные системные значения.	Форма Выбор системных значений
Подготовка к загрузке приложений	Создайте профайлы владельцев. Загрузите приложения. Перед тем как выполнять последующие шаги, убедитесь, что в системе существуют библиотеки и объекты приложений.	Форма Установка приложения
Настройка групп пользователей	Создайте описания заданий, библиотеки групп и профайлы групп.	Форма Описание группы пользователей
Настройка отдельных пользователей	Создайте библиотеки и профайлы пользователей	Форма Профайл пользователя

Таблица 60. Этапы настройки защиты ресурсов

Этап	Ваши действия	Необходимые формы
Настройка принадлежности и общих прав доступа	Установите принадлежность библиотек и объектов и задайте общие права доступа к ним.	Форма Установка приложения
Создание списка прав доступа	Создайте списки прав доступа.	Форма Список прав доступа
Настройка специальных прав доступа	Задайте права доступа к библиотекам и отдельным объектам.	Форма Описание библиотеки
Защита вывода на принтер	Создайте очереди вывода и назначьте устройство для вывода.	Форма Защита рабочей станции и очереди вывода
Защита для рабочих станций	Установите защиту рабочих станций.	Форма Защита рабочей станции и очереди вывода

Дополнительная информация по управлению защитой системы приведена в разделах:

- Тестирование защиты.
- Изменение информации о защите.
- Сохранение информации о защите.
- Контроль защиты.

Перед тем как начать

Если вы устанавливаете новую систему, то перед настройкой защиты выполните следующие действия:

- Убедитесь в том, что системный блок и другие устройства установлены и работают правильно. Если вы не планируете присваивать устройствам имена в соответствии с соглашениями, принятыми в системе iSeries, то подключайте рабочие станции и принтеры только после того, как вы измените системное значение, определяющее правила присвоения имен устройствам (QDEVNAMING). Когда именно подключать устройства, указано в разделе Применение новых системных значений.
- Загрузите лицензионные программы, с которыми вы планируете работать.

Настройка общих параметров среды

Перед тем как задать пользовательские параметры защиты, необходимо полностью настроить общую системную среду. Этот раздел поможет вам задать системные значения и создать собственный пользовательский профайл с помощью меню SETUP (Настройка). Вы также сможете изменить ИД и пароли пользователей для профайлов Специальных сервисных средств (DST).

В приведенных ниже описаниях процедур вы найдете примеры вывода различных команд. Учтите, что будет показан не весь экран, а только та информацию, которая необходима для выполнения задачи.

Какие формы вам потребуются?

Используйте информацию, которую вы ввели в форме ″Выбор системных значений″ во время планирования общей стратегии защиты.

Для настройки общих параметров среды необходимо выполнить следующие задачи:

1. Вход в систему.
2. Выбор требуемого уровня поддержки.
3. Запрет на вход в систему других пользователей.
4. Задание системных значений защиты.
5. Применение новых системных значений.
6. Создание профайла системного администратора

Выполнив описанные выше действия, смените пароли DST, чтобы предотвратить их неправильное использование. Более подробная информация приведена в разделе Специальные сервисные средства.

Вход в систему

Для того чтобы начать настройку системной среды, необходимо войти в систему.

1. Войдите в систему с консоли как системный администратор (QSECOFR). При первом входе в систему введите пароль QSECOFR. Срок действия этого пароля, поставляемого с системой, через некоторое время истечет, и система выдаст приглашение на изменение пароля. Для успешного входа в систему необходимо ввести новый пароль.
2. В поле *Меню* экрана входа в систему укажите `SETUP`.

Примечание: Меню SETUP полностью называется Настройка системы, пользователей и устройств. В данном тексте упоминается как Настройка.

```
                Вход в систему
                             Система . . . . .
                             Подсистема. . . .
                             Дисплей . . . . .

Пользователь. . . . . .  QSECOFR
Пароль    . . . . . .  _________
Программа/процедура . . . . . .  _________
Меню  . . . . . .  SETUP
Текущая библиотека. . . . . .  _________
```

После входа в систему вы должны выбрать требуемый уровень поддержки.

Выбор требуемого уровня поддержки

После входа в систему вы должны выбрать требуемый уровень поддержки для пользователей. **Уровень поддержки** определяет объем информации, показываемой на экране. Многие системные меню существует в двух вариантах.

- Меню для основного уровня поддержки содержит меньше информации, и в нем не применяется техническая терминология.
- В меню для промежуточного уровня поддержки показано больше информации с использованием технических терминов.

Набор показываемых полей или доступных функций зависит от варианта меню. Наши инструкции помогут вам выбрать версию меню для работы. Для изменения уровня поддержки нажмите клавишу **F21** (Выбрать уровень поддержки). **F21** доступна не из всех меню.

После выбора уровня поддержки вы должны запретить вход в систему для других пользователей на время настройки параметров защиты.

Запрет на вход в систему других пользователей

После выбора уровня поддержки вы должны запретить другим пользователям вход в систему. Если вы опасаетесь, что другие пользователи могут вмешаться в работу системы до того, как вы настроите ее защиту, вы можете запретить им доступ с других рабочих станций. Однако это необязательный этап. Выполняйте его только в том случае, если считаете необходимым:

1. В меню Настройка нажмите **F9** для перехода к командной строке
2. В командной строке введите `GO DEVICESTS`.
3. Появится меню Задачи состояния устройства. Если появится меню Работа с состоянием конфигурации нажмите **F21** (Выбрать уровень поддержки) и выберите основной уровень поддержки.
4. Выберите опцию **1** (Работа с дисплейными устройствами).
5. В меню Работа с дисплейными устройствами сделайте все рабочие станции, кроме той, с которой вы сейчас работаете, недоступными. Для этого введите **2** перед именем каждой рабочей станции и нажмите клавишу **Enter**.
6. Для возврата к меню Настройка дважды нажмите **F3** (Выход).
7. Для завершения работы с командной строкой нажмите **F12** (Отмена).

```
                          Работа с дисплейными устройствами

Введите опции и нажмите Enter.
  1=Сделать доступным   2=Сделать недоступным  5=Показать
  7=Показать сообщение  8=Работа с контроллером и линией
  13=Изменить описание

Опц  Устройство  Тип     Состояние
__   DSP01       3196    QSECOFR
2_   DSP02       3196    Доступно для работы
2_   DSP03       3196    Доступно для работы
2_   DSP04       3196    Доступно для работы
```

В устройстве, которое вы сделали недоступным, меню входа в систему отсутствует даже после его включения. Такое состояние сохраняется до перезагрузки системы. Возможно, вам потребуется повторить этот этап.

Запретив другим пользователям входить в систему, вы можете задать системные значения защиты.

Задание системных значений защиты

После установки запрета на вход в систему других пользователей следует задать системные значения.

Введите информацию в полях Части 1 формы Выбор системных значений:

1. В меню Настройка выберите опцию **1** (Изменить системные опции).
2. Введите в меню Изменить системные опции информацию из формы Выбор системных значений. Те значения, которые вы не хотите изменять, можно пропустить с помощью клавиши Tab.
3. Если системные время и дата не были заданы при запуске системы, введите в этом меню правильные значения.
4. После ввода информации на этой странице, перейдите к следующей странице с помощью клавиши Page down. Слово *Еще...* в правом нижнем углу экрана означает, что меню показано на экране не целиком.

```
                            Изменить системные опции
Система:
Введите варианты, нажмите Enter.

Имя системы . . . . . .   JKLTOY     Имя

Опции даты и времени:
  Системная дата. . . . . .   09/21/99     ММ/ДД/ГГ
  Системное время . . . . . .   10:52:57     ЧЧ:ММ:СС
  Разделитель даты  . . . . . .   1            1=/
                                               2=-
                                               3=.
                                               4=,
                                               5=пробел
  Формат даты . . . . . .   МДГ          ГМД, МДГ, ДМГ, ЮЛ
  Разделитель времени . . . . .   1            1=:
                                               2=.
                                               3=,
                                               4=пробел


                                                                      Еще...
F1=Справка  F3=Выход   F5=Обновить  F12=Отмена
```

5. Введите варианты на второй странице меню и нажмите клавишу Page down.

```
                          Изменить системные опции

Введите варианты, нажмите Enter.

Опции защиты:
  Уровень защиты  . . . . . .   40
   :
   :
  Разрешить системным администраторам
    входить в систему с любой дисплейной
    станции . . . . . .   H
```

6. Введите варианты на третьей странице меню и нажмите клавишу **Enter**.

```
                          Изменить системные опции

Введите варианты, нажмите Enter.

Опции устройства:
  Формат присвоения имен новым
  устройствам  . . . . . .   1


  Принтер по умолчанию  . . . .   PRT01

Дополнительные опции:
  Поместить пользователей в среду
    S/36 при входе в систему. .   H
  Сохранить информацию учета для
    завершенных заданий с
    выводом на принтер  . . . .   Д
```

7. Снова появится меню Настройка. В нижней части экрана будет показано сообщение: **Системные опции успешно изменены. Выполните IPL**.

   Примечание: Система запрашивает IPL только в том случае, если был изменен уровень защиты.

В конце большинства разделов, связанных с системными задачами, приведена таблица с описанием возможных ошибок и действий по их исправлению. Эти таблицы помогут в том случае, если результаты ваших действий будут отличаться от описанных в этом руководстве. Эти таблицы могут содержать сведения не о всех неполадках. Их назначение - указать вам путь решения проблемы и упростить работу с системой.

Возможная ошибка	Исправление
Появилось Главное меню AS/400.	Вы нажали **F3** (Выход) или **F12** (Отмена). Введите GO SETUP и повторите описанные здесь действия.
Появилось другое меню, например, Изменить опции очистки.	Вы выбрали неверную опцию в меню Настройка. Нажмите **F3** (Выход) для возврата к меню и повторите попытку.
После нажатия клавиши **Enter** опять появилось меню Изменить системные опции.	Прочитайте сообщение об ошибке, показанное в нижней части экрана. Возможно, вы ввели недопустимое значение. Если вам потребуется дополнительная информация, нажмите **F1** (Справка). Если вы хотите восстановить исходные значения измененных вами полей, нажмите **F5** (Обновить). Повторите попытку.
Вы нажали клавишу **Enter**, введя в меню не все значения.	Вы можете вызывать это меню для изменения системных значений столько раз, сколько необходимо. Выберите опцию **1** в меню Настройка и введите значения, пропущенные в предыдущий раз. **Внимание: Не изменяйте уровень защиты в рабочей системе, не посоветовавшись предварительно со специалистом. Также не изменяйте имя системы, если вы работаете с iSeries Access или соединены с другим компьютером.**

Возможная ошибка	Исправление
Вместо клавиши Page Down вы нажали **Enter**.	Выберите опцию **1** в меню Настройка и нажмите Page Down для перехода ко второй странице. Введите нужные варианты и нажмите клавишу **Enter**.

После ввода информации вы должны применить новые системные значения.

Применение новых системных значений

После ввода системных значений необходимо применить некоторые из этих значений. Большинство системных значений после изменения вступают в силу немедленно. Новый уровень защиты системы будет установлен только после перезагрузки системы. Убедитесь, что вы ввели все значения в меню Изменить системные опции правильно, и примените новые значения.

Примечание: Подключите к системе рабочие станции, если вы не выполнили этого ранее. При запуске системы эти устройства будут автоматически добавлены в конфигурацию в соответствии с форматом присвоения имен, выбранным вами в меню Изменить системные опции.

Выключите систему и запустите ее повторно, следуя описанным ниже инструкциям. После запуска системы введенные вами в меню Изменить системные опции значения вступят в силу.

1. Вы должны войти в систему с консоли, другие рабочие станции подключать нельзя.
2. Убедитесь, что переключатель режима на системном блоке находится в положении Normal.
3. В меню Настройка выберите опцию Задачи включения и выключения питания.
4. Выберите опцию Немедленно выключить питание системы, а затем включить его. Нажмите клавишу **Enter**.
5. Появится приглашение подтвердить запрос на выключение. Нажмите **F16** (Подтвердить).

Система автоматически перезагрузится. Экран в течение нескольких минут будет пуст. После этого повторно появится меню Вход в систему.

После применения новых системных значений вы должны создать профайл системного администратора для себя.

Создание профайла системного администратора

Системный администратор - это пользователь, входящий в класс *SECOFR или обладающий специальными правами *ALLOBJ и *SECADM.

После применения системных значений, введенных в меню Изменить системные опции, создайте пользовательские профайлы для себя и своего заместителя. Рекомендуется использовать для выполнения функций системного администратора именно этот профайл, а не QSECOFR.

1. Войдите в систему как QSECOFR и вызовите меню SETUP.

   В правом верхнем углу меню Вход в систему показано имя системы.

```
                Вход в систему
                           Система . . . . .
                           Подсистема. . . .
                           Дисплей . . . . .

Пользователь. . . . . .  QSECOFR
Пароль    . . . . . .    __________
Программа/процедура . .  __________
Меню  . . . . . .  . .   SETUP
Текущая библиотека. . .  __________
```

2. В меню Настройка выберите опцию *Работа с регистрацией пользователей*. В меню Работа с регистрацией пользователей перечислены все профайлы в системе.

   Примечание: Если появится меню Работа с пользовательскими профайлами, нажмите **F21** (Выбрать уровень поддержки) и выберите основной уровень поддержки.

3. Для создания нового профайла введите **1** (Добавить) в колонке *Опц* и имя профайла в колонке *Пользователь*. Нажмите клавишу **Enter**.

```
                          Работа с регистрацией пользователей

Введите опции и нажмите Enter.
  1=Добавить 2=Изменить 3=Копировать 4=Удалить 5=Показать

Опц     Пользователь       Описание
1       JONESS
QDOC                           Профайл для работы с документами
QSECOFR                        Профайл системного администратора
```

4. В меню Добавить пользователя задайте свой пароль.
5. Введите в показанных в примере полях нужную информацию.
6. Нажмите клавишу Page down для перехода к следующей странице меню.

```
                          Добавить пользователя

Введите варианты, нажмите Enter.

Пользователь. . . . . .   JONESS
Описание пользователя . .   Jones, Sharon
Пароль    . . . . . .   secret
Тип пользователя. . . . .   *SECOFR
Группа        . . . . . .   *NONE

Ограничение на ввод команд  _____
Библиотека по умолчанию .
Принтер по умолчанию. . .   *WRKSTN
Начальная программа . . .   *NONE
Библиотека  . . . . . .

Начальное меню  . . . .
Библиотека  . . . . . .
```

7. Введите нужную информацию в полях на второй странице меню и нажмите клавишу **Enter**.
8. Убедитесь, что в нижней строке меню Работа с регистрацией пользователей показано подтверждающее сообщение.
9. Нажмите **F3** (Выход) для возврата к меню Настройка.

```
                          Добавить пользователя

Введите варианты, нажмите Enter.

Обработка Attention . . .   *SYSVAL
  Библиотека. . . . . .
```

Возможная ошибка	Исправление
Вы нажали клавишу **Enter**, введя не все значения.	Выберите опцию *Изменить* в меню Работа с регистрацией пользователей для изменения созданного профайла. Если профайл не показан в списке, нажмите **F5** (Обновить), затем найдите его, листая список с помощью клавиши Page down.

После того как вы создали себе профайл системного администратора, вы должны изменить ИД пользователя и пароли пользователей DST. Более подробная информация о сервисных средствах приведена в разделе Специальные сервисные средства справочной системы Information Center.

Задание системных значений защиты

В этом разделе описано, как с помощью команды Работа с системными значениями (WRKSYSVAL) изменять и просматривать системные значения.

Какие формы вам потребуются?

Используйте информацию, которую вы ввели в форме ″Выбор системных значений″ во время планирования общей стратегии защиты.

Для настройки системных значений выполните следующие задачи:

1. Изменение системных значений защиты.
2. Изменение отдельных системных значений.

Войдите в систему

При входе в систему укажите следующую информацию:

Профайл
Ваш профайл (потребуются права доступа *SECADM и *ALLOBJ)

Меню MAIN

Войдя в систему, вы можете приступать к изменению системных значений защиты.

Изменение системных значений защиты

Войдя в систему, выполните следующую процедуру для задания системных значений защиты, указанных в Части 2 формы Выбор системных значений.

1. Введите `WRKSYSVAL *SEC` в командной строке и нажмите клавишу **Enter**. Параметр *SEC означает, что вы хотите работать только с системными значениями, определяющими защиту системы.
2. В меню Работа с системными значениями введите **2** (Изменить) в колонке *Опция* перед именем системного значения, которое вы хотите изменить. Если требуемое системное значение не показано на экране, просмотрите весь список с помощью клавиши Page down.

```
                        Работа с системными значениями

Поместить на   . . . . .              Первый символ
Подмножество     . . . .   *SEC       F4 для списка

Введите опции и нажмите Enter.
  2=Изменить  5=Показать

        Системное
Опция   значение    Тип         Описание
        QINACTMSGQ  *SEC        Очередь сообщений неактивных заданий
2       QLMTDEVSSN  *SEC        Ограничить сеансы устройств
        QLMTSECOFR  *SEC        Ограничить доступ для системного администратора
        QMAXSGNACN  *SEC        Действие при ошибке входа в систему
  ⋮
```

3. Введите для системного значения нужный вариант и нажмите **Enter**. На экране опять появится меню Работа с системными значениями.

```
                        Изменить системное значение
Системное значение . . :    QLMTDEVSSN
Описание     . . . . . :    Ограничить сеансы устройств


Введите значение, нажмите Enter.

  Ограничить сеансы устройств  0           0=Не ограничивать
                                           1=Ограничить
```

4. Убедитесь, что в нижней строке экрана показано сообщение об успешном выполнении операции.

Возможная ошибка	**Исправление**
Показаны не те системные значения, которые которые показаны здесь.	Вы не указали параметр *SEC. Сравните значение поля *Подмножество* в верхней части меню с полем в примере. Поместите курсор на поле *Подмножество*. Введите *SEC и нажмите клавишу **Enter**.
Система не выполняет команду. На экране показано прежнее меню.	Прочитайте сообщение об ошибке в нижней части меню. Возможно, вы неверно ввели имя команды. Повторите попытку. Если в сообщении указано, что у вас нет прав доступа, выйдите из системы и войдите с профайлом системного администратора.
После нажатия клавиши **Enter** опять появилось меню Изменить системное значение.	Прочитайте сообщение об ошибке в нижней части экрана. Возможно, вы ввели неверное или недопустимое значение. Для получения дополнительной информации нажмите **F1** (Справка).
Вместо меню Работа с системными значениями показано другое меню.	Возможно, вы нажали **Enter** дважды. Введите WRKSYSVAL *SEC.
Вы выбрали системное значение, которое не хотите изменять.	Нажмите **F12** (Отмена) для возврата к меню Работа с системными значениями.

Что означает символ * (звездочка)?

Как вы могли заметить, перед некоторыми значениями показана звездочка (*). Этот символ применяется в системе для того, чтобы отличать специальные значения от обычных слов. Например, *NONE в качестве пароля пользовательского профайла означает, что никто не сможет войти в систему с таким профайлом. Для того чтобы задать в качестве пароля слово NONE, вы должны ввести символы NONE.

При настройке защиты системы обращайте особое внимание на использование ″звездочки″ в инструкциях и формах.

После изменения системных значений защиты вы можете изменить другие необходимые значения.

Изменение отдельных системных значений

После изменения системных значений защиты вы можете изменить другие необходимые значения.

Например, системное значение Тайм-аут отключенного задания (QDSCJOBITV) не является системным значением защиты. Оно не входит в подмножество *SEC в меню Работа с системными значениями. Вы можете изменить QDSCJOBITV (или любое другое системное значение) следующим образом:

1. Введите `WRKSYSVAL QDSCJOBITV` и нажмите клавишу **Enter**.
2. В меню Работа с системными значениями введите **2** (Изменить) в колонке *Опция* перед именем QDSCJOBITV.
3. Введите нужное значение QDSCJOBITV.
4. Проверьте наличие сообщения с подтверждением.

```
                          Изменить системное значение
Системное значение . . :   QDSCJOBITV
Описание     . . . . . :   Тайм-аут отключенного задания


Введите значение, нажмите Enter.

  Тайм-аут отключенного задания      ..... 300
```

Печать списка значений защиты

После ввода всей информации из формы Выбор системных значений вы можете напечатать список всех системных значений защиты. Введите `WRKSYSVAL *SEC OUTPUT(*PRINT)`. Храните копию списка вместе с формой Выбор системных значений. После каждого изменения системных значений защиты создавайте этот список повторно.

После ввода информации из формы Выбор системных значений для всех системных значений вы можете загрузить свои приложения.

Организация защиты при загрузке приложений

После задания системных значений вы можете подготовить систему к загрузке необходимых приложений. В этом разделе описаны действия по настройке защиты, которые необходимо выполнить при загрузке в систему библиотек приложений. После создания профайлов и других объектов защиты, обратитесь к разделам ″Настройка принадлежности и общих прав доступа″ и ″Настройка защиты ресурсов″, в которых описан выбор владельцев и прав доступа приложений.

По возможности библиотеки приложений рекомендуется загружать в систему до настройки групп пользователей и отдельных профайлов. При создании описаний заданий и профайлов вы должны будете указать объекты приложений.

Если приложения не будут предварительно установлены, то при настройке будут появляться сообщения-предупреждения, например, такие:

- При создании описаний заданий не удалось найти начальные библиотеки.
- При создании профайлов не удалось найти начальные библиотеки.

Вы не сможете протестировать описания заданий и профайлы до тех пор, пока в системе не будут установлены библиотеки приложений.

Используйте формы Установка приложений, подготовленные вами при планировании установки приложений.

Для каждого приложения выполните следующие задачи:

1. Создайте профайл владельца.
2. Загрузите приложение.

Вход в систему

- Для создания профайла владельца:

  Профайл
  Ваш профайл (необходимы права доступа *SECADM)

  Меню MAIN

- Для загрузки библиотек приложений:

  Уточните у поставщика приложения, под управлением какого профайла вы должны войти в систему для загрузки приложения: как системный администратор или как владелец приложения.

Войдя в систему, вы можете создать профайл владельца приложений.

Создание профайла владельца

Войдя в систему, обратитесь к Плану установки приложений и выясните, нужно ли создать какие-либо профайлы перед загрузкой приложения. Для создания профайла:

1. Введите команду CRTUSRPRF (Создать пользовательский профайл) и нажмите **F4** (Приглашение).
2. В меню Создать пользовательский профайл укажите необходимые значения полей, следуя инструкциям специалиста или поставщика приложения.
3. Нажмите **F10** (Дополнительные поля) и с помощью клавиши Page Pown перейдите к следующей странице меню.

```
                      Создать пользовательский профайл (CRTUSRPRF)

Введите варианты, нажмите Enter.

Профайл пользователя . . . . . >
Пароль пользователя. . . . . .   *USRPRF
Задать истечение срока пароля. .   *NO
Состояние. . . . . .   *ENABLED
Класс пользователя . . . . . .   *USER
Уровень поддержки  . . . . . .   *SYSVAL
Текущая библиотека . . . . . .   *CRTDFT
Начальная программа  . . . . . .   *NONE
  Библиотека . . . . . .
Начальное меню . . . . . .   MAIN
  Библиотека . . . . . .     *LIBL
Ограничить возможности . . . . .   *NO
Описание     . . . . . .   Владелец xxxxxx
```

4. Проверьте наличие сообщений в нижней строке меню.

Примечание: В разделе Создание профайла группы создание профайлов описано более подробно.

После создания владельца приложения вы можете приступать к загрузке приложения.

Загрузка приложения

Загрузите библиотеки приложений, следуя инструкциям поставщика приложения. В разделе ″Настройка принадлежности и общих прав доступа″ приведены сведения, которые помогут вам выбрать владельца и задать общие права доступа к приложению.

После загрузки всех приложений вы можете перейти к настройке групп пользователей.

Настройка групп пользователей

После выполнения всех необходимых действий по настройке защиты при загрузке приложений вы можете приступать к настройке групп пользователей. Вам надо создать библиотеки групп, описания заданий и профайлы групп. Последовательно выполняя инструкции данного раздела, настройте одну из групп пользователей, потом вернитесь в начало и повторите эти действия для других групп. В приведенном примере используется информация из формы Описание группы пользователей для торгового отдела и для склада фирмы JKL Toys.

Воспользуйтесь формами Описание группы пользователей, подготовленными при планировании групп пользователей.″

Для настройки групп пользователей выполните следующие задачи:

1. Создание библиотеки для группы пользователей.
2. Создание описания задания.
3. Создание профайла группы.

Вход в систему

Профайл
Ваш профайл (необходимы права доступа *SECADM)

Меню MAIN

После входа в систему создайте библиотеку для группы пользователей.

Создание библиотеки для группы

Войдя в систему, создайте библиотеку для группы пользователей. Если вы планируете задать для группы общую библиотеку, в которой будут храниться создаваемые этой группой объекты (например программы Query), то эту библиотеку необходимо создать до профайла группы:

1. Введите `CRTLIB` (Создать библиотеку) и нажмите **F4** (Приглашение).
2. Введите в меню требуемую информацию. Имя библиотеки должно совпадать с именем профайла группы.
3. Нажмите **F10** (Дополнительные параметры).
4. Задайте общие права доступа к библиотеке и создаваемым в ней новым объектам.
5. Нажмите клавишу **Enter**. Проверьте наличие сообщения с подтверждением.

```
                          Создать библиотеку

Введите варианты, нажмите Enter.

Библиотека . . . . . .   DPTWH
Тип библиотеки . . . . . .   *PROD
Описание   . . . . . .   Библиотека склада

                          Дополнительные параметры

Права доступа. . . . . .   *USE
ИД пула (ASP)  . . . . . .   1
Права доступа к созд. объектам . .   *CHANGE
Контроль за созд. объектов . . . .   *SYSVAL
```

Возможная ошибка	Исправление
Вы нажали клавишу **Enter**, не задав описание библиотеки.	Введите команду **CHGLIB** и нажмите **F4** (Приглашение). Укажите в приглашении имя библиотеки и нажмите **Enter**. В меню Изменить библиотеку задайте описание.
Вы указали неверное имя библиотеки.	Введите команду Переименовать объект (RNMOBJ).

После создания библиотеки для группы вы можете создать описание задания.

Создание описания задания

После создания библиотеки для группы, вы можете создать описание задания для каждой группы.

Если библиотеки, которые должны быть включены в начальный список библиотек, еще отсутствуют в системе, то при создании описаний заданий будут выданы предупреждающие сообщения.

1. Введите **CRTJOBD** (Создать описание задания) и нажмите **F4** (Приглашение).
2. Заполните следующие поля:

   Описание задания:
   Совпадает с именем профайла группы.

   Имя библиотеки:
   QGPL

   Текст:
   Описание группы
3. Нажмите **F10** (Дополнительные параметры).
4. С помощью клавиши Page Down перейдите к полю *Начальный список библиотек*.

```
                    Создать описание задания

Введите варианты, нажмите Enter.

Описание задания . . . . . .   DPTSM
  Библиотека . . . . . .   QGPL
Очередь заданий. . . . . .   QBATCH
  Библиотека . . . . . .     *LIBL
Приоритет задания (в JOBQ) . . . .   5
Приоритет вывода (а OUTQ)  . . . .   5
Печатающее устройство. . . . . .   *USRPRF
Очередь вывода . . . . . .   *USRPRF
  Библиотека . . . . . .
Описание   . . . . . .   Отдел продаж и маркетинга
```

5. В поле *Начальный список библиотек* замените значение *SYSVAL на **+** (плюс), означающий, что вы собираетесь ввести список значений. Нажмите клавишу **Enter**.

```
Код учета ресурсов. . . . . .   *USRPRF
   :
Проверка синтаксиса CL. . . . . .   *NOCHK
Начальный список библиотек. . . . .   +
              + для доп. значений
```

6. В поле *Начальный список начальных библиотек* введите имена библиотек, отмеченных (✓) в форме Описание группы пользователей:
   - Указывайте в каждой строке по одной библиотеке.
   - Включите в список библиотеки QGPL и QTEMP. Задания хранят в библиотеке QTEMP временные объекты. **Все начальные списки библиотек должны включать библиотеку QTEMP**. Для большинства приложений в начальном списке библиотек должна быть указана и библиотека QGPL.
   - Текущую библиотеку (по умолчанию) включать в список не обязательно. Она будет добавлена автоматически при следующем входе в систему.
7. Нажмите клавишу **Enter**. Проверьте наличие сообщений. (Для просмотра всех сообщений нажмите клавишу Page Down).

```
Задайте дополнительные значения

Введите варианты, нажмите Enter.

Список начальных библиотек . . .     CUSTLIB
                                     ITEMLIB
                                     COPGMLIB
                                     ICPGMLIB
                                     QGPL
                                     QTEMP
```

Возможная ошибка	Исправление
Вместо клавиши **F10** вы нажали **Enter**.	Для добавления нужных библиотек в список начальных библиотек введите команду **CHGJOBD** (Изменить описание задания) и нажмите **F4**.
При попытке создать описание задания появилось сообщение об ошибке.	Чаще всего ошибка возникает из-за того, что вы пытаетесь добавить в список библиотеку, еще не существующую в системе. Это предупреждающее сообщение. Несмотря на сообщение, описание задания будет создано и библиотека будет включена в начальный список библиотек. Однако до тех пор, пока указанная библиотека не будет создана, вы не сможете войти в систему с помощью профайла, в котором применяется это описание задания. Если же ошибка продолжает возникать даже после создания библиотеки, то, возможно, вы неверно указали ее имя. Проверьте правильность написания и повторите попытку.

После создания описания задания вы можете приступить к созданию профайла группы.

Создание профайла группы

После создания описания задания вы можете приступить к созданию профайла группы. Для этого вам потребуется информация из Части 2 формы Описание группы пользователей.

1. Вызовите команду Работа с пользовательскими профайлами: WRKUSRPRF *ALL. Первоначально в меню будет показан список профайлов, поставляемых фирмой IBM.

   Примечание: Если появится меню Работа с регистрацией пользователей, нажмите клавишу **F21** и выберите промежуточный уровень поддержки.

2. Для создания нового профайла введите **1** в колонке *Опц* (опция) и имя профайла в колонке *Профайл*. Нажмите клавишу **Enter**.

```
                        Работа с пользовательскими профайлами

Введите опции и нажмите Enter.
  1=Создать  2=Изменить  3=Копировать 4=Удалить  5=Показать
  12=Работа с объектами по владельцу


Опц  Профайл     Текст
1    DPTSM
     QDOC        Профайл для работы с документами
     QSECOFR     Профайл системного администратора
```

3. Укажите в полях ввода информацию из формы Описание группы пользователей.
4. Если вы хотите оставить в поле значение по умолчанию, пропустите его с помощью клавиши **Tab**.
5. Нажмите **F10** (Дополнительные параметры).
6. Нажмите Page Down.

```
                      Создать пользовательский профайл (CRTUSRPRF)

Введите варианты, нажмите Enter.

Профайл пользователя . . . . . > DPTSM
Пароль пользователя. . . . . .   *none
Задать истечение срока пароля. .   *NO
Состояние. . . . . .   *ENABLED
Класс пользователя . . . . . .   *USER
Уровень поддержки  . . . . . .   *SYSVAL
Текущая библиотека . . . . . .   *CRTDFT
Начальная программа  . . . . . .   cpsetup
  Библиотека . . . . . .   cppgmlib
Начальное меню . . . . . .   cpmain
  Библиотека . . . . . .   cppgmlib
Ограничить возможности . . . . .   *yes
Описание     . . . . . .   Отдел продаж и маркетинга
```

7. Введите дополнительных полях информацию из формы Описание группы пользователей и нажмите клавишу **Enter**.

```
                      Создать пользовательский профайл

                        Дополнительные параметры

Специальные права доступа. . . .   *USRCLS

   ⋮
Описание задания . . . . . .   DPTSM
  Библиотека . . . . . .   QGPL
```

```
                      Создать пользовательский профайл

Права доступа группы . . . . . *NONE

   ⋮
Устройство печати  . . . . . . . PRT03
```

8. Проверьте наличие сообщений.

Запомните

Профайл группы - это просто особый тип пользовательского профайла. Во многих сообщениях и меню, профайлы групп называются пользовательскими профайлами. Системе распознает профайл как профайл группы только после того, как вы добавите в него пользователей или присвоите этому профайлу идентификатор группы (gid).

Возможная ошибка	Исправление
Вы нажали клавишу **Enter**, не закончив ввод всех параметров профайла группы.	Нажмите **F5** (Обновить) для добавления созданного профайла в меню Работа с пользовательскими профайлами. Выберите опцию **2** (Изменить) и укажите необходимые параметры профайла.
Вы присвоили созданному профайлу неверное имя.	Переименовать профайл нельзя. Скопируйте профайл с помощью опции **3**, указав для нового профайла правильное имя. После этого удалите (опция **4**) профайл с неверным именем.
Некоторые поля формы Описание группы пользователей не показаны на экране.	Убедитесь, что вы работаете с промежуточным уровнем поддержки. При использовании основного уровня поддержки вместо меню Создать пользовательский профайл появляется меню Добавить пользователя. Нажмите **F12** (Отмена) для возврата к меню Работа с регистрацией пользователей. Нажмите **F21** и измените уровень поддержки. См. также раздел ″Выбор уровня поддержки.″
Вы случайно удалили значения по умолчанию в меню Создать пользовательский профайл.	Если вы оставите поле пустым, то при создании пользовательского профайла система присвоит соответствующему параметру значение по умолчанию. Если вы хотите просмотреть значения по умолчанию, нажмите **F5** (Обновить) для восстановления исходного вида всего меню. Введите информацию повторно.

Вывод результатов

С помощью команды Показать пользователей с правами доступа (DSPAUTUSR) просмотрите список имен и описаний всех профайлов. Введите команду `DSPAUTUSR OUTPUT(*PRINT)`. Убедитесь, что у всех профайлов в поле Пароль указано значение *NONE.

Перед настройкой профайлов отдельных пользователей выполните следующие действия:

- Создайте описание задания для каждой группы пользователей.
- Создайте библиотеку для каждой группы (необязательно).
- Создайте профайл для каждой группы пользователей.

Настройка профайлов отдельных пользователей

При настройке групп пользователей вы создали профайлы групп. Теперь необходимо создать профайлы отдельных пользователей, входящих в состав этих групп.

Последовательно выполняя инструкции данного раздела, создайте профайлы для пользователей одной из групп, потом вернитесь в начало и повторите эти действия для других групп. В приведенных примерах применяется пример формы Профайлы отдельных пользователей, подготовленной Шэрон Джонс для отдела продаж и маркетинга, а также для склада фирмы JKL Toys. Копии этих форм приведены в разделе ″Планирование профайлов отдельных пользователей.″

Воспользуйтесь формами Профайлы отдельных пользователей, которые вы подготовили на этапе ″Планирование профайлов отдельных пользователей.″

Для создания профайлов отдельных пользователей необходимо выполнить следующие задачи:

1. Создание личной библиотеки. (Необязательно.)
2. Копирование профайла группы.
3. Задание срока действия пароля.
4. Создание дополнительных профайлов пользователей. (Необязательно.)

   Примечание: Повторяя операции Создание личной библиотеки и Создание дополнительных профайлов пользователей, создайте пользовательский профайл для каждого члена группы.
5. При необходимости Измените информацию о пользователе.
6. Просмотрите результаты.

Вход в систему

Профайл
Ваш профайл (необходимы права доступа *SECADM)

Меню SETUP

Создание личной библиотеки

Перед настройкой профайлов отдельных пользователей может потребоваться создать для каждого из них личную библиотеку, в которой будут храниться объекты, например, программы Query. Личные библиотеки необходимо создать до создания профайлов отдельных пользователей.

1. Введите команду **CRTLIB** и нажмите **F4** (Приглашение).
2. Присвойте библиотеке имя, совпадающее с именем пользовательского профайла
3. Нажмите **F10** (Дополнительные параметры).
4. Задайте общие права доступа к библиотеке и создаваемым в ней новым объектам.
5. Нажмите клавишу **Enter**. Проверьте наличие сообщения с подтверждением.

```
                          Создать библиотеку

Введите варианты, нажмите Enter.

Библиотека . . . . . .   DPTSM
Тип библиотеки . . . . . .   *PROD
Описание   . . . . . .   Библиотека для склада

                         Дополнительные параметры

Права доступа. . . . . .   *EXCLUDE
ИД пула (ASP). . . . . .   1
Права доступа для соз. объектов.   *CHANGE
Контроль за созд. объектов . . .   *SYSVAL
```

После создания личной библиотеки вы можете создать отдельный пользовательский профайл, скопировав профайл группы.

Копирование профайла группы

Профайл группы выполняет в системе две основные функции:

1. С его помощью система определяет, есть ли у члена группы права доступа к объекту.
2. Профайл группы можно использовать как шаблон для создания отдельных пользовательских профайлов, входящих в данную группу.

При настройке групп пользователей вы создали профайлы групп. Теперь, скопировав профайл группы, вы можете создать профайл отдельного пользователя, а потом, копируя его, создать и другие профайлы.

1. Выберите в меню Настройка опцию Работа с регистрацией пользователей.

   Примечание: Если появится меню Работа с пользовательскими профайлами, нажмите **F21** (Выбрать уровень поддержки) и выберите основной уровень поддержки.
2. Введите **3** (Копировать) в колонке *Опц* рядом с именем группы пользователей. На экране появится меню Копировать пользователя. (Если нужная группа не показана на экране, пролистайте меню с помощью клавиши Page Down). Система укажет в полях ввода значения из скопированного профайла, оставив имя профайла пустым.

```
                          Работа с регистрацией пользователей

Введите опции и нажмите Enter.
  1=Добавить 2=Изменить 3=Копировать 4=Удалить 5=Показать

Опц     Профайл        Описание

        DPTSM          Отдел продаж и маркетинга
3       DPTWH          Склад
```

3. Введите имя и описание создаваемого пользовательского профайла.
4. Оставьте поле пароля пустым. Система автоматически присвоит профайлу пароль, совпадающий с его именем.
5. Укажите имя профайла группы в поле *Группа пользователей*.
6. С помощью формы Профайл отдельного пользователя выясните, нужно ли указать для данного пользователя какие-либо параметры, значения которых отличаются от значений для всей группы. Введите эти значения.
7. Нажмите Page Down.

```
                                Копировать пользователя

Копировать пользователя :   DPTWH

Введите варианты, нажмите Enter.

Пользователь. . . . . .   WILLISR
Описание пользователя . .   Роуз Уиллис
Пароль    . . . . . .
Тип пользователя. . . . .   *SYSOPR
Группа пользователя . . .   DPTWH

Ограничение на ввод команд  H

Библиотека по умолчанию .   DPTWH
Принтер по умолчанию. . .   PRT04
Начальная программа . . .   *NONE
  Библиотека. . . . . .

Начальное меню  . . . . .   ICMAIN
  Библиотека. . . . . .      ICPGMLIB
```

8. Внесите на следующей странице меню все необходимые изменения и нажмите клавишу **Enter**.
9. Найдите сообщение с подтверждением в нижней строке меню Работа с регистрацией пользователей.

```
                                Копировать пользователя

Копировать пользователя :   DPTWH

Введите варианты, нажмите Enter.

Обработка Attention . . .   *SYSVAL
  Библиотека. . . . . .
```

Возможная ошибка	Исправление
Вместо меню Копировать пользователя может появиться меню Создать пользовательский профайл.	Нажмите **F12** (Отмена) для возврата в меню Работа с пользовательскими профайлами. Нажмите **F21** и выберите основной уровень поддержки. Повторите операцию копирования.
Выбранное вами имя пользовательского профайла не помещается в приглашении.	Несмотря на то, что допустимая длина имени профайла равна 10 символам, меню Копировать пользователя и Добавить пользователя поддерживают только имена, длина которых не превышает 8 символов. Сократите имя или создавайте профайлы для отдельных пользователей с промежуточным уровнем поддержки.

Тестирование пользовательского профайла

Создав первый пользовательский профайл в группе следует проверить его работу, войдя в систему с помощью этого профайла. Убедитесь, что показано выбранное начальное меню и что запущена указанная начальная программа.

Если войти в систему с помощью этого профайла не удается, то, возможно, в системе не был найден один из указанных в профайле объектов: начальная программа, описание задания или одна из начальных библиотек. С помощью меню Работа с выводом на принтер найдите протокол задания, который был создан при попытке входа в систему. В нем перечислены все возникшие ошибки.

Информация о поиске и устранении неполадок, возникающих при изменении параметров защиты, приведена в разделе ″Проверка защиты.″

После проверки пользовательского профайла вы можете задать срок действия пароля.

Срок действия пароля

Укажите в пользовательских профайлах, что при первом входе в систему пользователь должен изменить пароль. На основном уровне поддержки поле *Задать срок действия пароля* показано не будет. После создания пользовательского профайла путем копирования его нужно будет изменить отдельно. Это можно сделать с помощью команды CHGUSRPRF *имя_профайла* PWDEXP(*YES).

Примечание: Если вы хотите войти в систему с помощью созданного профайла для его проверки, то сделайте это *до* задания срока действия пароля.

Возможная ошибка	Исправление
Вы тестировали профайл и вам пришлось изменить пароль.	Введите **CHGUSRPRF** *имя_профайла* и нажмите **F4** (Приглашение). Задайте пароль профайла, совпадающий с его именем. (Введите в поле Пароль имя профайла). Введите ***YES** в поле *Задать срок действия пароля*. Эту процедуру необходимо выполнять на промежуточном уровне поддержки.

После создания первого индивидуального пользовательского профайла вы можете создать дополнительные пользовательские профайлы.

Создание дополнительных пользовательских профайлов

После того как вы скопировали профайл группы и создали на его основе первый пользовательский профайл, вы можете создать дополнительные пользовательские профайлы. Для создания дополнительных профайлов скопируйте первый созданный пользовательский профайл. При создании профайлов с помощью функции копирования необходимо внимательно просматривать их значения. Изучите форму Профайл отдельного пользователя и убедитесь, что вы изменили все поля, уникальные для данного пользователя.

1. В меню Работа с регистрацией пользователей введите **3** (Копировать) напротив имени пользовательского профайла-образца.
2. В меню Копировать пользователя задайте имя и описание профайла.
3. Укажите в полях ввода информацию, уникальную для нового пользователя.

```
                          Работа с регистрацией пользователей

Введите опции и нажмите Enter.
  1=Добавить 2=Изменить 3=Копировать 4=Удалить 5=Показать

Опц     Профайл        Описание

        DPTSM          Отдел продаж и маркетинга
        DPTWH          Склад
3       WILLISR        Уиллис, Роуз
```

Возможная ошибка	Исправление
Профайл-образец не показан в меню Работа с регистрацией пользователей.	Нажмите **F5** (Обновить). Просмотрите список с помощью клавиш Page Up и Page Down. Список упорядочен в алфавитном порядке по именам профайлов.

Если вы хотите изменить какие-либо параметры профайла, просмотрите раздел Изменение информации о пользователе.

Изменение информации о пользователе

Иногда может потребоваться изменить информацию о пользователе, не показываемую в меню Копировать пользователя. Например, иногда нужно указать, что пользователь входит сразу в несколько групп (относится к нескольким профайлам групп). Вы можете изменить эту информацию после создания пользовательского профайла путем копирования.

1. В меню Работа с регистрацией пользователей нажмите **F21** и выберите промежуточный уровень поддержки.
2. В меню Работа с пользовательскими профайлами введите **2** (Изменить) в колонке *Опц* (опция) напротив имени профайла, который вы хотите изменить. Нажмите клавишу **Enter**.

```
                        Работа с пользовательскими профайлами

Введите опции, нажмите Enter.
  1=Создать  2=Изменить  3=Копировать 4=Удалить  5=Показать
  12=Работать с объектами по владельцу


Опц  Профайл     Текст
2    AMESJ       Эймис, Дженис
     DPTSM       Отдел продаж и маркетинга
     QDOC        Профайл для работы с документами
     QSECOFR     Профайл системного администратора
     WAGNERR     Вагнер, Рэй
     WILLISR     Уиллис, Роуз
```

3. В меню Изменить пользовательский профайл нажмите **F10** (Дополнительные параметры).
4. Пролистайте меню с помощью клавиши Page Down и найдите поля, которые нужно изменить. Например, если вы хотите добавить пользователя в другие группы, пролистайте меню до поля *Дополнительные группы*.
5. Введите нужные значения и нажмите **Enter**. Будет выдано сообщение с подтверждением и опять появится меню Работа с пользовательским профайлами.

```
                        Изменить пользовательский профайл (CHGUSRPRF)

Введите варианты, нажмите Enter.

Объем доступной памяти   . . . .   *NOMAX
Высший приоритет планирования. .   3
Описание задания . . . . . .       DPTWH
  Библиотека . . . . . .             QGPL
Профайл группы . . . . . .         DPTWH
Владелец . . . . . .               *GRPPRF
Права доступа группы . . . . . .   *USEE
Тип прав доступа группы. . . . .   *PGP
Дополнительные группы. . . . . .   DPTIC
               + для доп. значений
```

После изменения информации о пользователе вы можете просмотреть результаты для проверки профайла.

Просмотр пользовательских профайлов

Существует несколько способов просмотра созданных профайлов.

Просмотр отдельного профайла

Выберите опцию **5** (Показать) в меню Работа с регистрацией пользователей или в меню Работа с пользовательскими профайлами.

Вывод одного профайла

Введите команду Показать пользовательский профайл: DSPUSRPRF *имя_профайла* DETAIL(*BASIC) OUTPUT(*PRINT).

Просмотр элементов группы

Введите команду DSPUSRPRF *имя_профайла_группы* *GRPMBR. Для печати списка служит команда OUTPUT(*PRINT).

Просмотр всех профайлов

Для просмотра списка имен и описаний всех профайлов, упорядоченных по группам, вызовите команду Показать пользователей с правами доступа DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT) .

Перед настройкой принадлежности и общих прав доступа необходимо выполнить следующие задачи:

- Создать все отдельные пользовательские профайлы

- Задать срок действия пароля для каждого профайла.
- Напечатать список всех профайлов, упорядоченный по группам, и подшить его в одну папку с формами описания групп пользователей. После каждого добавления пользователей печатайте новую версию этого списка.

Настройка защиты ресурсов

Этот раздел поможет вам задать принадлежность и общие права доступа к объектам, а также особые права доступа к приложениям. Здесь также описаны действия по настройке защиты рабочих станций и принтеров. Последовательно выполните инструкции данного раздела для одной библиотеки, потом вернитесь в начало и повторите эти действия для других библиотек. После настройки защиты ресурсов для одного приложения, повторите эти же действия для других приложений.

Эти процедуры пригодятся вам как при установке нового приложения, так и при настройке защиты ресурсов уже существующего приложения.

В данном разделе используются примеры форм с описанием списков прав доступа, библиотек и очередей вывода фирмы JKL Toys. Примеры этих форм приведены в разделе ″Настройка принадлежности и общих прав доступа″.

Какие формы вам потребуются?

- Формы Установка приложений, подготовленные вами на этапе ″Планирование установки приложений.″
- Формы Списки прав доступа, подготовленные вами на этапе ″Планирование установки приложений.″
- Формы Описание библиотеки, подготовленные вами на этапе ″Планирование установки приложений.″
- Форма Защита очередей вывода и рабочих станций, подготовленная вами на этапе ″Защита вывода на принтер″ и ″Защита рабочих станций.″
- Форма Ответственные за работу системы, подготовленная вами во время ″Планирования общей стратегии защиты.″

Настроить защиту ресурсов можно несколькими способами. В этом разделе действия приведены в том порядке, в каком они перечислены в формах Установка приложений, Списки доступа и Описание библиотеки:

1. Настройка принадлежности и общих прав доступа.
2. Создание списков прав доступа.
3. Защита объектов с помощью списков прав доступа.
4. Добавление пользователей в списки прав доступа.
5. Настройка особых прав доступа.
6. Защита вывода на принтер.
7. Защита рабочих станций.
8. Ограничение доступа к очереди сообщений системного оператора.

Настройка принадлежности и общих прав доступа

Этот раздел поможет вам задать принадлежность и общие права доступа к библиотекам приложений, библиотекам групп и личным библиотекам. Последовательно выполните инструкции данного раздела для одного приложения, потом вернитесь в начало и повторите эти действия для всех остальных приложений. В качестве примеров в этом разделе приведены формы Установка приложения, подготовленные администратором компании JKL Toys Шэрон Джонс для приложения Заказы клиентов (этап ″Планирование установки приложений″).

Процедуры, описанные в этом разделе, относятся как к установке нового приложения, так и к настройке защиты уже существующего приложения.

Используйте формы Установка приложений, подготовленные вами при планировании установки приложений.

Перед настройкой принадлежности и общих прав доступа необходимо выполнить следующие задачи:

1. Создание профайла владельца.
2. Изменение принадлежности библиотеки.
3. Задание принадлежности объектов приложения.
4. Задание прав доступа к библиотеке.
5. Задание прав доступа ко всем объектам библиотеки.
6. Задание общих прав доступа к создаваемым объектам.
7. Работа с библиотеками групп и личными библиотеками.

Вход в систему

Профайл
Ваш профайл (необходимы права доступа *ALLOBJ)

Меню MAIN

Создание профайла владельца

Если профайл владельца не существует, выполните следующие действия:

- Введите команду CRTUSRPRF (Создать профайл владельца). В поле Пароль укажите *NONE.

Если профайл владельца уже существует, выполните следующие действия:

- Введите команду CHGUSRPRF (Изменить профайл владельца) и укажите в поле Пароль значение *NONE.

После создания профайла пользователя вы можете изменить владельца библиотеки.

Изменение принадлежности библиотеки

Эта команда изменяет принадлежность библиотеки, а не находящихся в ней объектов.

Внимание: Перед изменением принадлежности любого объекта приложения проконсультируйтесь с поставщиков приложения. В некоторых приложениях используются функции, для правильной работы которых необходимо, чтобы объект принадлежал определенному пользователю.

1. Введите CHGOBJOWN (Изменить владельца объекта) и нажмите **F4** (Приглашение).
2. Укажите имя библиотеки, тип объекта (*LIB) и нового владельца.
3. Проверьте наличие сообщений с подтверждением.

```
                      Изменить владельца объекта (CHGOBJOWN)

Введите варианты, нажмите Enter.

Объект . . . . . . . . . . . . . > COPGMLIB
  Библиотека . . . . . . . . . . >   *LIBL       Имя,
Тип объекта  . . . . . . . . . .> *LIB
Новый владелец . . . . . . . .   COWNER
Права дост. текущего владельца .   *REVOKE
```

Возможная ошибка	Исправление
Выдано сообщение об ошибке.	Чаще всего ошибка возникает из-за того, что библиотека или профайл нового владельца не найдены в системе. Проверьте правильность написания имен и повторите попытку.

После изменения принадлежности библиотеки вы можете задать принадлежность объектов приложения.

Задание принадлежности объектов приложения

Изменение принадлежности объектов приложений - это довольно сложная задача, так как ее требуется выполнять отдельно для каждого объекта. По возможности поручите задание принадлежности специалисту или поставщику приложения.

Просмотр списка объектов библиотеки

Перед изменения принадлежности напечатайте список всех объектов библиотеки с помощью команды Показать библиотеку. Вы можете использовать эту распечатку как справочную таблицу. Введите команду DSPLIB *имя_библиотеки* *PRINT.

Выбор способа

Выберите один из следующих способов изменения принадлежности объектов в библиотеках приложений:

Таблица 61. Способы изменения принадлежности объектов

Способ	Выполняемые действия	Условия применения
Команда Работа с объектами по владельцу	Показывает меню со списком всех объектов, принадлежащих профайлу. Изменение владельца объекта выполняется с помощью опции этого меню.	Это самый простой способ. Однако фирма IBM не рекомендует им пользоваться, если владельцем объектов является пользователь QPGMR или QSECOFR. Эти профайлы являются владельцами очень большого числа объектов, поэтому показанный список будет очень велик.
Команда Изменить принадлежность объекта	Для каждого объекта требуется вызов отдельной команды. Однако с помощью клавиши *Восстановить* (**F9**) вы можете повторять предыдущую команду и не вводить ее каждый раз.	Если владельцем объектов является пользователь QPGMR или QSECOFR, то этот способ позволит быстрей изменить принадлежность объектов.

Применение команды Работа с объектами по владельцу (WRKOBJOWN): Это способ рекомендуется применять для изменения принадлежности объектов в том случае, когда профайлы, поставляемые фирмой IBM, *не* являются владельцами объектов:

1. Введите WRKOBJOWN *имя-профайла-владельца*. На экране появится список всех объектов, принадлежащих данному профайлу.
2. Введите опцию **9** (Изменить владельца) напротив имен всех объектов библиотеки, принадлежность которых вы хотите изменить.
3. В строке *Параметры или команда*, расположенной в нижней части меню, введите NEWOWN(*имя-профайла-владельца*) и нажмите клавишу **Enter**.
4. Владельцем всех выбранных объектов станет профайл, указанный вами в нижней строке. В нижней части меню появится сообщение с подтверждением. Выбранные объекты будут удалены из показанного списка, так как они больше не принадлежат данному профайлу.
5. Повторите действия 2 и 4 до тех пор пока не будет изменена принадлежность всех нужных объектов библиотеки.

```
                          Работа с объектами по владельцу

Пользовательский профайл . :   OLDOWNER

Введите опции и нажмите Enter.
  2=Редактировать права доступа   4=Удалить  5=Показать права доступа
  8=Показать описание             9=Изменить владельца

Опц  Объект        Библиотеки    Тип       Атрибут
     COPGMMSG      COPGMLIB      *MSGQ
9    CUSTMAS       CUSTLIB       *FILE
9    CUSTMSGQ      CUSTLIB       *MSGQ
     ITEMMSGQ      ITEMLIB       *MSGQ


   ⋮

Параметры или команда
===> NEWOWN(COWNER)
F3=Выход  F4=Приглашение  F5=Обновить   F9=Восстановить
F18=Конец
```

Возможная ошибка	Исправление
Появилось меню Изменить владельца объекта.	Это меню будет показано в том случае, если вы указали опцию **9** (Изменить владельца), но не указали имя нового владельца в нижней строке меню Работа с объектами по владельцу, либо указали имя неправильно. Нажмите **F12** (Отмена) для возврата к меню Работа с объектами по владельцу. Повторите попытку. Убедитесь, что вы ввели параметры именно так, как это показано в примере.

Для изменения принадлежности объектов, владельцами которых является профайл QPGMR или QSECOFR, вы можете воспользоваться командой Изменить владельца объекта.

Применение команды Изменить владельца объекта: Это способ рекомендуется применять для изменения принадлежности объектов в том случае, когда владельцем объектов *является* профайл QPGMR или QSECOFR.

1. Введите CHGOBJOWN и нажмите **F4** (Приглашение).
2. Укажите в полях ввода информацию о первом объекте списка и нажмите клавишу **Enter**.

```
                      Изменить владельца объекта (CHGOBJOWN)

Введите варианты, нажмите Enter.

Объект . . . . . . . . . . . . . > CUSTMAS
  Библиотека . . . . . . . . . . >   CUSTLIB
Тип объекта  . . . . . . . . . . > *FILE
Новый владелец . . . . . . . . .   COWNER
Права дост. текущего владельца .   *REVOKE
```

3. Появится сообщение, подтверждающее изменение принадлежности объекта. Вычеркните этот объект из списка.
4. Нажмите **F9** (Восстановить) для повтора введенной ранее команды.
5. Нажмите **F4** (Приглашение). В меню Изменить владельца объекта введите информацию о следующем объекте и нажмите клавишу **Enter**.
6. Повторите четвертое и пятое действие для каждого объекта библиотеки.

Проверка результатов

Для того чтобы проверить, правильно ли изменена принадлежность объектов библиотеки, введите команду Работа с объектами по владельцу. Введите WRKOBJOWN *новый-профайл-владельца*. Сравните содержимое меню со списком объектов в библиотеке.

После изменения принадлежности объектов вы можете задать общие права доступа к библиотеке.

Задание прав доступа к библиотеке

После задания принадлежности объектов приложений, вы можете изменить общие права доступа к библиотеке с помощью команды Редактировать права доступа к объекту (EDTOBJAUT):

1. Введите EDTOBJAUT *имя_библиотеки* *LIB.
2. Переместите курсор вниз, на строку, в которой показано значение **PUBLIC*.
3. Укажите общие права доступа к библиотеке и нажмите клавишу **Enter**.

```
                          Редактировать права доступа к объекту

Объект . . . . . :   CUSTLIB         Владелец . . . . . :   COWNER
  Библиотека . . . :     QSYS        Основная группа. . . :   *NONE
Тип объекта  . . . :   *LIB

Внесите необходимые изменения и нажмите Enter.

  Объект защищен списком прав доступа   . . . . . .   *NONE

                        Права доступа
Пользователь Группа     к объекту
COWNER                  *ALL
*PUBLIC                 *CHANGE
```

4. В этом окне показаны новые права доступа.

Теперь вы можете задать права доступа ко всем объектам библиотеки.

Задание прав доступа ко всем объектам библиотеки

Для удаления текущих прав доступа к объектам библиотеки введите команду Аннулировать права доступа к объекту (RVKOBJAUT). Для задания общих прав доступа ко всем объектам библиотеки введите команду Предоставить права доступа к объекту (GRTOBJAUT):

1. Введите RVKOBJAUT и нажмите **F4** (Приглашение).
2. Укажите в полях ввода приведенную ниже информацию, указав нужное имя библиотеки приложений, и нажмите клавишу **Enter**.

```
                    Аннулировать права доступа к объекту (RVKOBJAUT)

Введите варианты, нажмите Enter.

Объект . . . . . .   *all
  Библиотека . . . . . .     custlib
Тип объекта  . . . . . .   *all
Пользователи . . . . . .   *public
               + для доп. значений
Права доступа  . . . . . .   *all
```

Примечание: Если в библиотеке находится много объектов, то для обработки запроса системе может потребоваться несколько минут.

3. Введите GRTOBJAUT и нажмите **F4** (Приглашение).
4. Укажите в полях ввода приведенную ниже информацию, указав нужное имя библиотеки приложений и требуемые права доступа, а затем нажмите клавишу **Enter**.

```
                    Предоставить права доступа к объекту (GRTOBJAUT)

Введите варианты, нажмите Enter.

Объект . . . . . .   *all
  Библиотека . . . . . .    custlib
Тип объекта  . . . . . .   *all
Пользователи . . . . . .   *public
               + для доп. значений
Права доступа  . . . . . .   *use
```

Примечание: Если в библиотеке находится много объектов, то для обработки запроса системе может потребоваться несколько минут.

После задания общих прав доступа ко всем объектам библиотеки вы можете проверить результаты с помощью протокола задания.

Проверка результатов с помощью протокола задания: После вызова команды GRTOBJAUT для изменения прав доступа к нескольким объектам вы можете просмотреть протокол задания и проверить, были ли внесены необходимые изменения.

1. Введите DSPJOBLOG (Показать протокол задания).
2. Нажмите **F10** (Показать подробные сообщения).
3. Для каждого объекта библиотеки должно быть выдано сообщение об изменении прав доступа. Найдя сообщение для объекта, вычеркивайте этот объект из списка.

```
                          Показать все сообщения
Система:  RCHASxxx
Задание :   QPADEV0010    Польз.  :   JCHEIDEL       Номер . . . :   025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  Права доступа предоставлены пользователю *PUBLIC к объекту CUSTMAS в
     CUSTLIB с типом
    *FILE.
  Права доступа предоставлены пользователю *PUBLIC к объекту CUSTMSGQ в
     CUSTLIB с типом
    *MSGQ.
  Предоставлены права доступа к 2 объектам. Не предоставлены к 0 объектам.
     Частично предоставлены к 0
    объектам.
  Права доступа к объекту предоставлены.
7>> dspjoblog
```

Возможная ошибка	Исправление
В протоколе задания указано, что права доступа к некоторым объектам библиотеки не изменены.	Для получения дополнительной информации о сообщении поместите курсор на сообщение и нажмите **F1**. Для задания прав доступа к указанным объектам воспользуйтесь командой EDTOBJAUT.

Теперь вы можете задать общие права доступа к создаваемым объектам.

Задание общих прав доступа к создаваемым объектам

Описание библиотеки включает параметр Права доступа к создаваемым объектам (CRTAUT), определяющий общие права доступа к объектам, создаваемым в библиотеке. При создании в библиотеке нового объекта для него по умолчанию указываются права данные, заданные в параметре CRTAUT библиотеки. В этом параметре рекомендуется указывать значение, совпадающее с общими правами доступа к большинству хранящихся в библиотеке объектов.

1. Введите CHGLIB *имя-библиотеки* и нажмите **F4** (Приглашение).
2. Нажмите **F10** (Дополнительные параметры).
3. Введите значение в поле *Права доступа к создаваемым объектам*.

```
                     Изменить библиотеку (CHGLIB)

Введите варианты, нажмите Enter.

Библиотека . . . . . . . . . . . > CUSTLIB
Тип библиотеки . . . . . . . . .   *PROD
Описание   . . . . . . . . . . .   'Информация о заказчиках'


                    Дополнительные параметры

Права доступа к созд. объектам .   *CHANGE
Контроль за созд. объектов . . .   *SYSVAL
```

Если вы укажете в параметре CRTAUT значение *SYSVAL, то при создании в библиотеке нового объекта система будет применять текущую настройку системного значения QCRTAUT. Для того чтобы изменение системного значения QCRTAUT не влияло на права доступа пользователей, укажете для каждой библиотеки в параметре CRTAUT конкретные права доступа.

Теперь вы можете работать с библиотеками групп и личными библиотеками.

Работа с библиотеками групп и личными библиотеками

Вашему профайлу принадлежат библиотеки групп и личные библиотеки, созданные при настройке групп пользователей и отдельных пользователей.

С помощью описанных выше процедур вы можете передать принадлежность библиотеки группы профайлу группы, а принадлежность личной библиотеки - отдельному пользовательскому профайлу. Введите команду EDTOBJAUT.

Укажите общие права доступа ко всем создаваемым объектам в личной библиотеке или в библиотеке группы, задав для каждой библиотеки параметр Права доступа к создаваемым объектам. Введите команду CHGLIB.

Перед созданием списков прав доступа необходимо выполнить следующие задачи:

- Просмотрите формы Установка приложения и Описание библиотеки и убедитесь, что вы задали принадлежность и общие права доступа для всех библиотек приложений.
- Задайте принадлежность и права доступа к создаваемым объектам для всех созданных библиотек групп и личных библиотек.

Примечание: Вы можете напечатать список всех библиотек с помощью команды DSPOBJD *ALL *LIB *PRINT.

Создание списка прав доступа

Выполнив настройку принадлежности и общих прав доступа, вы можете приступать к созданию списков прав доступа. С помощью информации, указанной в формах Список прав доступа, создайте все списки прав доступа, необходимые для защиты библиотеки. Введите команду Создать список прав доступа (CRTAUTL):

1. Введите CRTAUTL и нажмите **F4** (Приглашение).
2. Введите информацию, указанную в форме Список прав доступа.
3. Нажмите **F10** (Дополнительные параметры).

4. Дополнительные параметры позволяют задать общие права доступа к объектам, защищенным с помощью данного списка прав доступа.
5. Проверьте наличие сообщения с подтверждением.

```
                    Создать список прав доступа (CRTAUTL)

Введите варианты, нажмите Enter.

Список прав доступа. . . . . .   custlst1
Описание           . . . . . .   Удаление файлов

                         Дополнительные параметры

Права доступа. . . . . . . . . .   *ALL
```

Возможная ошибка	Исправление
Вы неверно указали имя списка прав доступа.	После создания списка прав доступа переименовать его нельзя. Удалите список командой DLTAUTL и создайте его заново.
Вы забыли задать для списка общие права доступа.	Введите команду Редактировать список прав доступа (EDTAUTL).

Теперь вы можете настроить защиту объектов с помощью созданного списка прав доступа.

Защита объектов с помощью списка прав доступа

После создания списка прав доступа введите команду Редактировать права доступа к объекту (EDTOBJAUT); эта команда позволит вам настроить защиту объектов, перечисленных в форме Список прав доступа:

1. Введите EDTOBJAUT и нажмите **F4** (Приглашение).
2. Укажите необходимую информацию в полях ввода и нажмите клавишу **Enter**.
3. В меню Редактировать права доступа к объекту укажите имя списка прав доступа.
4. Если общие права доступа к объекту заданы в списке прав доступа, то укажите в соответствующем параметре значение *AUTL.
5. Повторите эти действия для всех объектов, указанных в форме Список прав доступа.

```
                          Редактировать права доступа к объекту

Объект . . . . . :   ARFILE01        Владелец . . . . . :   OWNAR
  Библиотека . . . :     CUSTLIB     Основная группа. . . :   *NONE
Тип объекта  . . . :   *FILE

Внесите необходимые изменения и нажмите Enter.

  Объект, защищенный списком прав доступа . . . . . .   CUSTLST1

                          Права доступа
Пользователь Группа      к объекту
OWNER                    *ALL
*PUBLIC                  *AUTL
```

Теперь вы можете добавить пользователей в список прав доступа.

Добавление пользователей в список прав доступа

После защиты объектов с помощью списка прав доступа введите команду Редактировать список прав доступа (EDTAUTL) и добавьте в список прав доступа пользователей, перечисленных в форме Список прав доступа.

1. Введите EDTAUTL *имя_списка*.
2. В меню Редактировать список прав доступа нажмите **F6** (Добавить пользователей).
3. Введите имена пользователей или групп и укажите предоставленные им права доступа, после чего нажмите клавишу **Enter**.
4. Эти имена должны появиться в списке.

```
                            Добавить пользователей

Объект . . . . . :   WSLST1          Владелец .
  Библиотека . . . :     QSYS

Укажите новых пользователей и нажмите Enter.

             Права дост.  Управление
Профайл      к объекту    списком
QSECOFR     *CHANGE
```

Возможная ошибка	Исправление
Вы предоставили пользователю или группе неверные права доступа.	Изменить права доступа можно с помощью меню Редактировать список прав доступа.
Вы ошибочно добавили в список пользователя или группу.	Вы можете удалить пользователя или группу с помощью команды Удалить запись списка прав доступа (RMVAUTLE), либо перейти в меню Редактировать список прав доступа и указать в поле прав доступа этого пользователя (группы) пустое значение (пробелы).

Проверка результатов

Введите команду Показать список прав доступа (DSPAUTL) для просмотра прав доступа всех пользователей, указанных в данном списке. Для просмотра перечня всех объектов, защищенных данным списком, нажмите **F15**.

Перед настройкой особых прав доступа необходимо выполнить следующие задачи:

- С помощью команды CRTAUTL создайте все необходимые для приложения списки прав доступа.
- С помощью команды EDTOBJAUT настройте защиту объектов с помощью списка прав доступа.
- С помощью команды EDTAUTL добавьте пользователей в списки прав доступа.

Задание особых прав доступа

В разделе ″Настройка принадлежности и общих прав доступа″ описано применение команды GRTOBJAUT для настройки общих прав доступа ко всем объектам библиотеки с использованием информации из части 1 формы Описание библиотеки. Теперь с помощью команды Редактировать права доступа к объекту (EDTOBJAUT) вы можете задать особые права доступа к библиотеке и ее объектам, используя информацию из части 2 формы Описание библиотеки.

Дополнительная информация о настройке особых прав доступа приведена в разделах:

- Настройка особых прав доступа к библиотеке.
- Настройка особых прав доступа к объекту.

- настройка прав доступа к нескольким объектам одновременно.

Настройка особых прав доступа к библиотеке

Библиотека представляет собой один из типов объектов. Права доступа к библиотеке задаются так же, как и для любого другого объекта, с помощью команды EDTOBJAUT. Все библиотеки хранятся в библиотеке QSYS, поставляемой фирмой IBM. В следующем примере меню применяется информация из части 2 формы Описание библиотеки для библиотеки CONTRACTS фирмы JKL Toys:

Показать особые права доступа к объектам библиотеки				
Профайл пользователя или группы	Имя объекта	Тип объекта	Требуемые права доступа	Список прав доступа
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

1. Введите EDTOBJAUT и нажмите **F4** (Приглашение).
2. Укажите необходимую информацию в полях ввода и нажмите клавишу **Enter**.

```
                    Редактировать права доступа (EDTOBJAUT)

Введите варианты, нажмите Enter.

Объект . . . . . .   CONTRACTS
  Библиотека . . . . . .    QSYS
Тип объекта  . . . . . .   *LIB
```

3. Для того чтобы предоставить права доступа пользователям, не указанным в списке, нажмите **F6** (Добавить пользователей) в меню Редактировать список прав доступа.
4. Нажмите клавишу **Enter**.

```
                            Добавить пользователей

Объект . . . . . :   CONTRACTS       Владелец . . . . . :   OWNCP
  Библиотека . . . . :    QSYS       Основная группа. . . :   *NONE
Тип объекта  . . . . :   *LIB


Укажите новых пользователей и нажмите Enter.

           Права доступа
Профайл    к объекту
DPTSM      *USE
DPTMG      *USE
```

5. Информация в меню Редактировать права доступа к объекту должна соответствовать частям 1 и 2 формы Описание библиотеки.

```
                          Редактировать права доступа к объекту

Объект . . . . . :   CONTRACTS       Владелец . . . . . :   OWNCP
  Библиотека . . . :     QSYS        Основная группа. . . :   *NONE
Тип объекта  . . . :   *LIB

Внесите необходимые изменения и нажмите Enter.

  Объект защищен списком прав доступа   . . . . . .   *NONE

                         Права доступа
Пользователь Группа      к объекту
OWNCP                    *ALL
DPTSM                    *USE
DPTMG                    *USE
*PUBLIC                  *EXCLUDE
```

Общие права доступа к новым объектам (CRTAUT) не показаны в меню Редактировать права доступа для библиотеки. Просмотреть права доступа CRTAUT для библиотеки можно с помощью команды Показать библиотеку (DSPLIB).

Эта процедура позволяет также задать особые права доступа к объекту системы.

Теперь вы можете настроить особые права доступа к объектам.

Настройка особых прав доступа к объекту

Особые права доступа к объекту в библиотеке приложения задаются так же, как и права доступа к самой библиотеке. В приведенном примере используется информация из части 2 формы Описание библиотеки для библиотеки COPGMLIB фирмы JKL Toys:

Таблица 62. форма Описание библиотеки фирмы JKL Toys

Профайл пользователя или группы	Имя объекта	Тип объекта	Требуемые права доступа	Список прав доступа
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. Введите EDTOBJAUT и нажмите **F4** (Приглашение).
2. Укажите необходимую информацию в полях ввода и нажмите клавишу **Enter**.
3. Введите информацию о правах доступа в меню Редактировать права доступа к объекту и нажмите клавишу **Enter**.

```
                          Редактировать права доступа к объекту

Объект . . . . . :   COMSGQ01        Владелец . . . . . :   OWNCO
  Библиотека . . . :     COPGMLIB    Основная группа  . . :   *NONE
Тип объекта  . . . :   *MSGQ

Внесите необходимые изменения и нажмите Enter.

  Объект защищен списком прав доступа   . . . . . .   *NONE

                         Права доступа
Пользователь Группа      к объекту
OWNCO                    *ALL
*PUBLIC                  *CHANGE
```

Теперь вы можете настроить права доступа к нескольким объектам.

Настройка прав доступа к нескольким объектам одновременно

В предыдущих примерах было показано, как настроить права доступа к отдельному объекту с помощью команды EDTOBJAUT. С помощью команды Предоставить права доступа (GRTOBJAUT) вы можете настроить защиту сразу для нескольких объектов. Введите GRTOBJAUT и нажмите **F4** (Приглашение). В приведенных ниже примерах показано, как изменить права доступа сразу для нескольких объектов.

- Указанные в этом примере значения задают общие права доступа *CHANGE ко всем очередям сообщений в библиотеке CUSTLIB.

```
                    Предоставить права доступа к объекту (GRTOBJAUT)

Введите варианты, нажмите Enter.

Объект . . . . . .   *all
  Библиотека . . . . . .    custlib
Тип объекта  . . . . . .   *msgq
Пользователи . . . . . .   *public
              + для доп. значений
Права доступа. . . . . .   *change
```

- В следующем примере показано, как предоставить пользователю AMES права доступа *ALL ко всем файлам библиотеки CUSTLIB, имена которых начинаются с символов WRK.

```
                    Предоставить права доступа к объекту

Введите варианты, нажмите Enter.

Объект . . . . . .   WRK*
  Библиотека . . . . . .    custlib
Тип объекта  . . . . . .   *file
Пользователи . . . . . .   AMES
              + для доп. значений
Права доступа  . . . . . .   *all
```

В этом примере имена объектов задавались с помощью **шаблонов**. Во многих командах в качестве имени объекта можно указывать первые символы этого имени со звездочкой (*). Система выполнит заданную операцию для всех объектов, имена которых начинаются с указанных символов. Параметры, для которых можно задавать шаблоны имен, перечислены в электронной справке по команде.

- Например, для того, чтобы защитить с помощью списка прав доступа ARLST1 все файлы, имена которых начинаются с символов AR, и указать, что общие права доступа к этим файлам должны быть взяты из списка, необходимо выполнить следующие два действия. Последовательность действий проиллюстрирована в приведенных ниже примерах меню.

```
                    Предоставить права доступа к объекту

Введите варианты, нажмите Enter.

Объект . . . . . .   AR*
  Библиотека . . . . . .    CUSTLIB
Тип объекта  . . . . . .   *FILE

   ⋮
Список прав доступа. . . . . .   ARLST1
```

```
                    Предоставить права доступа к объекту

Введите варианты, нажмите Enter.

Объект . . . . . .   AR*
  Библиотека . . . . . .     CUSTLIB
Тип объекта  . . . . . .   *FILE
Пользователь . . . . . .   *PUBLIC
               + для доп. значений
Права доступа. . . . . .   *AUTL
               + для доп. значений
```

Введите команду DSPJOBLOG в формате, описанном в разделе ″Проверка результатов с помощью протокола задания″ и убедитесь, что система выполнила запрошенное изменение прав доступа.

Перед тем как приступить к настройке защиты вывода на принтер, введите команду EDTOBJAUT или GRTOBJAUT и задайте особые права доступа в соответствии с информацией из части 2 формы Описание библиотеки.

Защита вывода на принтер

После задания особых прав доступа вы можете установить защиту конфиденциальной информации, выводимой на принтер; для этого необходимо выполнить инструкции описанные в следующих разделах:

- Создание очереди вывода и задание ограничений на работу с ней.
- Направление специального вывода на принтер в эту очередь.

Создание очереди вывода

1. Введите CRTOUTQ (Создать очередь вывода) и нажмите **F4** (Приглашение).
2. Укажите библиотеку и имя очереди вывода.
3. Нажмите **F10** (Дополнительные параметры).
4. С помощью клавиши Page Down найдите информацию о защите очереди вывода.

```
                    Создать очередь вывода (CRTOUTQ)

Введите варианты, нажмите Enter.

Очередь вывода . . . . . >   NEWCP
  Библиотека . . . . . .       CONTRACTS
Макс. размер буферного файла:
  Число страниц    . . . . . .   *NONE         Число, *NONE
  Начальное время. . . . . .                  Время
  Конечное время . . . . . .                  Время
            + для доп. значений
Порядок файлов в очереди . . . .   *FIFO
Удаленная система  . . . . . .   *NONE

   ⋮
Описание           . . . . . .   Очередь новых контрактов
```

5. Для предоставления необходимых прав доступа пользователям, которые будут работать с этой очередью и обслуживать ее, введите информацию из формы Защита очередей вывода и рабочих станций.
6. Нажмите клавишу **Enter** и проверьте наличие сообщения с подтверждением.

```
                    Создать очередь вывода (CRTOUTQ)

Введите варианты, нажмите Enter.


Дополнительные параметры

Показывать все файлы . . . . . *NO
Разделители заданий  . . . . . 0
Управляется оператором . . . . . *NO
Очередь данных . . . . . *NONE
  Библиотека . . . . . .
Права доступа для проверки . . . *OWNER
Права доступа. . . . . *LIBCRTAUT
```

Возможная ошибка	Исправление
Вместо клавиши **F10** вы нажали **Enter**.	Для ввода дополнительной информации введите команду Изменить очередь вывода (CHGOUTQ).
Вы создали очередь ввода в неверной библиотеке.	Введите команду Переместить объект (MOVOBJ) и укажите нужное имя библиотеки.

Теперь вы можете направить вывод на принтер в созданную очередь вывода.

Направление вывода на принтер в очередь вывода

Создав очередь вывода, вы можете направить в нее вывод на принтер. Назначение вывода на принтер обычно указывается в файле принтера. Узнайте у поставщика приложения имена и библиотеки файлов принтера для конфиденциальных отчетов.

Если эта информация вам недоступна, напечатайте отчет и заблокируйте его в очереди вывода. С помощью опции Атрибуты в меню Работа с буферными файлами определите имя файла принтера. Имя файла принтера показано в поле *Файл устройства* в меню Работа с атрибутами буферного файла.

Для изменения очереди вывода, связанной с файлом принтера, введите команду Изменить файл принтера (CHGPRTF):

```
CHGPRTF FILE(имя-библиотеки/имя-файла-принтера)
        OUTQ(имя-библиотеки/имя-очереди-вывода)
```

При следующем запросе отчет будет направлен в новую очередь вывода. Для перемещения буферного файла в другую очередь вывода выберите в меню Работа с буферными файлами опцию Изменить.

Допустим, Шэрон Джонс, системный администратор фирмы JKL Toys, хочет, чтобы прейскуранты, направляемые на принтера PRCLST1, хранились в очереди вывода PRICEQ. В этом случае необходимо ввести следующую команду:

```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

Для направления в очередь вывода PRICEQ всех отчетов с прейскурантами Шэрон может указать шаблон имени файла принтера:

```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

Для направления всех новых контрактов в очередь вывода NEWCP Шэрон может изменить очередь вывода, связанную с образцом документа, применяемым для создания контрактов.

Проверка результатов

Лучший способ проверить стратегию защиты конфиденциального вывода на принтер - это напечатать его. Проверьте, в какую очередь направляется вывод. Войдите в систему с помощью профайла системного оператора и проверьте, можете ли вы просматривать файлы в этой очереди или работать с ними.

Перед переходом к настройке защиты рабочих станций должны быть выполнены следующие задачи:

- С помощью команды CRTOUTQ должны быть созданы все очереди вывода, перечисленные в форме Защита очередей вывода и рабочих станций.
- Вывод на принтер должен быть связан с новыми очередями вывода с помощью команды CHGPRTF.

Защита рабочих станций

После настройки защиты вывода на принтер необходимо обеспечить защиту рабочих станций. Права доступа к рабочим станциям задаются так же, как к другим объектам системы. Вы можете предоставить пользователям права доступа к рабочим станциям с помощью команды EDTOBJAUT.

Для входа в систему с рабочих станций пользователям необходимы права доступа *CHANGE. Если системное значение QLMTSECOFR отлично от (0), то системный администратор или другой пользователь с правами доступа *ALLOBJ сможет входить в систему с любой рабочей станции.

Если системное значение QLMTSECOFR равно 1, то настройка прав доступа к рабочим станциям выполняется в соответствии со следующими принципами:

Пользователи, которым разрешено входить в систему с рабочей станции	Общие права доступа	Права QSECOFR	Права доступа отдельных пользователей
Все пользователи	*CHANGE	*CHANGE	Не требуются
Выбранные пользователи	*EXCLUDE	Нет прав доступа	*CHANGE
Выбранные пользователи и пользователи с правами доступа ко всем объектам	*EXCLUDE	*CHANGE	*CHANGE
Все пользователи, кроме пользователей с правами доступа ко всем объектам	*CHANGE	Нет прав доступа	Не требуются

Перед заданием ограничения доступа к очереди сообщений системного оператора введите команду EDTOBJAUT и установите защиту рабочих станций, используя информацию из формы Защита очередей вывода и рабочих станций.

Ограничение доступа к очереди сообщений системного оператора

Вы можете повысить надежность защиты, установив защиту вывода на принтер, защиту рабочих станций и ограничив доступ к очереди сообщений системного оператора.

Опция обработки сообщения в меню Операционная поддержка (ASSIST) позволяет пользователям просматривать очередь сообщений системного оператора (QSYSOPR) с помощью функциональных клавиш. Неверный ответ на сообщения системного оператора может привести к возникновению неполадок в системе. Для ответа на сообщения и их удаления из очереди пользователям необходимы права доступа *CHANGE. Такие права доступа должны быть только у системных операторов. Пользователи, которым разрешено иметь права доступа *CHANGE, перечислены в форме Ответственные за работу системы.

Введите команду EDTOBJAUT:

1. Введите `EDTOBJAUT QSYSOPR *MSGQ` и нажмите клавишу **Enter**.
2. Для просмотра подробной информации о правах доступа к объекту нажмите клавишу **F11**.
3. Задайте общие права доступа *OBJOPR, как показано в примере меню, и нажмите клавишу **Enter**.

```
                          Редактировать права доступа к объекту

Объект . . . . . :   QSYSOPR         Владелец . . . . . :   QSYS
  Библиотека . . . . :     QSYS      Основная группа. . . :   *NONE
Тип объекта  . . . . :   *MSGQ

Внесите необходимые изменения и нажмите Enter.

  Объект защищен списком прав доступа   . . . . . .   *NONE

                        Права дост.  ----------Объект-----------
Профайл    Группа     к объекту    Опер.  Упр.  Существ.  Измен.  Обращ.
*PUBLIC                 USER DEF          X
```

4. Система изменит значение, показанное в колонке *Права доступа к объекту*, на USER DEF (пользовательские).
5. Повторно нажмите **F11** для просмотра подробной информации о правах доступа.
6. Задайте общие права доступа *ADD, как показано в примере меню, и нажмите клавишу **Enter**.

```
                          Редактировать права доступа к объекту

Объект . . . . . :   QSYSOPR         Владелец . . . . . :   QSYS
  Библиотека . . . . :     QSYS      Основная группа. . . :   *NONE
Тип объекта  . . . . :   *MSGQ

Внесите необходимые изменения и нажмите Enter.

  Объект защищен списком прав доступа   . . . . . .   *NONE

                        Права доступа  ---------------Данные-------------
Профайл     Группа  к объекту      Чтен.  Доб.  Обнов.  Удал.  Выполн.
*PUBLIC                 USER DEF          X
```

7. Нажмите **F6** (Добавить пользователей) и добавьте пользователей, которые должны отвечать на сообщения QSYSOPR. Укажите для них права доступа *CHANGE.

Внимание: Не задавайте общие права доступа *EXCLUDE. Все задания (и пользователи) должны иметь права на добавление сообщений в очередь сообщений QSYSOPR.

Для того чтобы проверить правильность защиты ресурсов, выполните следующие действия:

- С помощью форм Список прав доступа и Описание библиотеки убедитесь, что вы настроили защиту всех библиотек приложений.
- С помощью форм Защита очередей вывода и рабочих станций убедитесь, что рабочие станции защищены, а специальные очереди вывода созданы.
- Ограничьте доступ к очереди сообщений системного оператора (QSYSOPR).
- Сохраните библиотеки приложений в соответствии с инструкциями, поставляемыми с приложениями. Информация о принадлежности и общих правах доступа хранится в системе вместе с приложением.
- Введите команду Сохранить данные о защите (SAVSECDTA) и сохраните резервную копию созданной информации о защите. Дополнительная информация об этой процедуре приведена в разделе ″Сохранение информации о защите″.

Теперь вы можете начать тестирование защиты.

Тестирование защиты

В этом разделе описаны способы тестирования защиты после настройки. При тестировании проверяется правильность работы всех настроек. Способы оценки эффективности защиты описаны в разделе ″Контроль защиты″.

Тестирование защиты следует выполнять после каждого серьезного изменения конфигурации системы, например, после добавления приложения, настройки защиты ресурсов для существующего приложения, добавления новой группы пользователей или изменения уровня защиты.

В следующих разделах описаны способы тестирования и диагностики неполадок, возникающих при изменении параметров защиты:

- Тестирование пользовательских профайлов.
- Тестирование защиты ресурсов.

Тестирование пользовательских профайлов

Тестирование защиты обычно начинают с проверки пользовательских профайлов, созданных после добавления в систему новой группы. Протестируйте отдельный пользовательский профайл, созданный путем копирования профайла группы.

- Можете ли вы войти в систему с помощью этого профайла? В случае неудачи просмотрите протокол задания, создаваемый при попытке входа в систему. Для поиска информации в протоколе задания выберите в меню операционной поддержки (ASSIST) опцию Работа с выводом на принтер.

  Наиболее вероятные причины сбоя:

  – Не найден один из обязательных объектов, например, начальное меню, текущая библиотека или начальная программа.
  – Ошибки связаны с указанным в описании задания списком библиотек. Либо одна из перечисленных библиотек не существует, либо вы забыли включить в этот список QGPL и QTEMP.
  – У пользователя нет прав доступа к рабочей станции.
- Было ли после входа в систему показано заданное начальное меню и была ли запущена начальная программа?
- Что произошло после того, как вы указали начальное меню или текущую библиотеку в меню входа в систему? Если для пользовательского профайла была задана опция ограничения возможностей (*YES), то должно появиться сообщение об ошибке.
- Появляется после нажатия клавиши Attention меню, указанное в пользовательском профайле?
- Направляется ли вывод на указанный в профайле принтер? Если нет, выберите в меню операционной поддержки (ASSIST) опцию Работа с выводом на принтер и определите, куда был направлен вывод. Найдите ошибку в пользовательском профайле или в описании задания.
- Доступна ли командная строка?
- Может ли приложение выполнять все необходимые функции без возникновения ошибок защиты? Подробные сведения приведены в разделе ″Тестирование защиты ресурсов″.
- Можете ли вы выполнять необходимые системные задачи, такие как управление принтерами или сохранение библиотек?

Если при входе в систему с помощью тестируемого профайла система потребует сменить пароль, не забудьте после завершения тестирования опять указать для профайла пароль, совпадающий с именем профайла:

1. Войдите в систему под управлением своего профайла (с правами доступа системного администратора).
2. Введите `CHGUSRPRF` *`имя-профайла`* `PASSWORD(`*`имя-профайла`*`) PWDEXP(*YES)`.

После проверки пользовательских профайлов вы можете приступить к тестированию защиты ресурсов.

Тестирование защиты ресурсов

После тестирования пользовательских профайлов следует также проверить защиту ресурсов. При этом следует обратить особое внимание на наличие следующих категорий пользователей:

- Пользователи, права доступа которых недостаточны для выполнения всех необходимых функций.
- Пользователи, у которых больше прав доступа, чем предполагалось.

Проверка достаточности прав доступа

Проверьте, достаточно ли у пользователя прав доступа на использование всех необходимых интерактивных и пакетных функций.

Тестирование интерактивных функций

Для проверки защиты ресурсов приложения потребуется войти в систему несколько раз с помощью разных профайлов. При работе с этими профайлами вы должны проверить, достаточно ли предоставленных им прав доступа для выполнения всех необходимых операций.

- Проверьте работу функций, для выполнения которых требуются права доступа различных уровней: для просмотра, изменения и удаления.
- Запустите несколько программ. Простого просмотра меню или выбора опции меню может оказаться недостаточно для проверки прав доступа. Иногда система обращается к файлу только после того, как вы фактически попытаетесь выполнить над ним какую-либо операцию, например, удаление записи. Проверка прав доступа выполняется при открытии файла. При этом в приложение передается сигнал об открытии.
- Сохраните записи об ошибках защиты. При возникновении ошибки на экране появится сообщение об отсутствии необходимых прав доступа к объекту с указанием имени этого объекта.

Тестирование пакетных функций

- Запустите из приложения какие-либо пакетные задания, используя профайлы пользователей, которые будут впоследствии работать с этими заданиями.
- Протестируйте пакетные задания, для выполнения которых требуются права доступа различного уровня: печать информации, изменение информации или удаление файлов.
- Проверьте, были ли зарегистрированы ошибки защиты в очереди сообщений QSYSOPR и в протоколе QHST. Просмотреть протокол QHST можно с помощью команды DSPLOG. Идентификаторы сообщений о защите лежат в следующих диапазонах: CPF2200, CPI2200, CPC2200, CPD2200, CPF4A00, CPI4A00, CPC4A00 и CPD4A00.

  Кроме того, для регистрации ошибок прав доступа и других событий защиты вы можете воспользоваться функцией контроля защиты.

Выявление избыточных прав доступа

После настройки защиты ресурсов для обеспечения сохранности секретной информации проверьте надежность этой защиты, используя несколько различных пользовательских профайлов. Войдите в систему с помощью профайла пользователя, который не должен иметь доступа к защищенной информации.

- Можете ли вы перейти в меню, из которого доступен защищенный файл?
- Что происходит при выборе опции меню, вызывающей действие над этим файлом?
- Доступна ли командная строка?
- Можете ли вы вызвать команду просмотра файла, например `CPYF FROMFILE(`*`имя_файла`*`) TOFILE(QSYSPRT)`?
- Можете ли вы просмотреть файл с помощью средств создания запросов?

В результате тестирования может оказаться, что вам необходимо изменить информацию о защите.

Изменение информации о защите

Теперь, когда вы составили план защиты вашей системы, вы должны убедиться, что он остается эффективным по мере роста и развития вашей организации.

В данном разделе основное внимание уделяется простоте как наилучшему средству достижения эффективности защиты. Вы использовали профайлы групп в качестве образцов для профайлов отдельных

пользователей. Вы получили представление об удобстве работы с общими правами доступа, списками прав доступа и правами доступа к библиотеке по сравнению с применением частных прав доступа. Тот же подход следует применять и при управлении защитой:

- При добавлении новой группы пользователей или нового приложения действуйте по той же схеме, что и при планировании защиты.
- Если вам потребовалось внести изменения в параметры защиты, постарайтесь придерживаться единого подхода в решении подобных задач вместо того, чтобы каждый раз придумывать нестандартные приемы.

В разделе Команды защиты перечислены команды для просмотра, изменения и удаления информации о защите.

В следующих разделах предложены варианты выполнения некоторых задач:

- Добавление пользователя в систему.
- Создание новой группы пользователей.
- Изменение группы пользователей.
- Добавление нового приложения.
- Добавление новой рабочей станции.
- Изменение полномочий пользователя.
- Удаление пользователя из системы.

Команды защиты

В приведенной ниже таблице перечислены команды, применяемые при работе с объектами защиты системы. Эти команды служат для выполнения следующих задач:

- Вывод и просмотр информации о защите.
- Изменение информации о защите.
- Удаление информации о защите.

Таблица 63. Команды защиты

Объект защиты	Способ просмотра	Способ изменения	Способ удаления
Системное значение	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	Нельзя удалить
Описание задания	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
Профайл группы	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1],[2]
Профайл пользователя	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]
Права доступа к объекту	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
Принадлежность объекта	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN позволяет аннулировать права предыдущего владельца
Основная группа	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP задает для основной группы значение *NONE

Таблица 63. Команды защиты (продолжение)

Объект защиты	Способ просмотра	Способ изменения	Способ удаления
Контроль за объектом	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (задать равным *NONE) CHGAUD
Список прав доступа	DSPAUTL DSPAUTLOBJ	EDTAUTL (права доступа пользователя к списку) EDTOBJAUT (объект защищен списком) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (весь список)[3] RMVAUTLE (удалить права доступа пользователя из списка) EDTOBJAUT (объект защищен диском) RVKOBJAUT

1. Если вам нужно удалить профайл, фирма IBM рекомендует выбрать опцию удаления в меню Работа с регистрацией пользователей. Эта опция позволяет удалять любые объекты, принадлежащие профайлу, или изменять их принадлежность. Специальные параметры команды DLTUSRPRF позволяют удалить все объекты, принадлежащие некоторому пользователю, или изменить их принадлежность. Вы не можете удалить профайл, пока он является владельцем объектов. Вы также не можете удалить профайл, являющийся основной группой для объектов.
2. Вы не можете удалить профайл непустой группы. Просмотреть список членов группы можно с помощью опции *GRPMBR команды DSPUSRPRF. Перед удалением профайла группы измените поле *профайл группы* во всех профайлах ее членов.
3. Вы не можете удалить список прав доступа, которым защищены объекты. Для просмотра списка объектов, защищенных списком, служит команда DSPAUTLOBJ. Измените права доступа к объектам, защищенным списком, с помощью команды EDTOBJAUT.

Вывод и просмотр информации и защите

Вы можете вывести на экран информацию о защите с помощью команды просмотра (DSP) с опцией печати (*PRINT). Например, если вы хотите просмотреть содержимое списка прав доступа с именем MYLIST, введите `DSPAUTL MYLIST *PRINT`.

У некоторых команд просмотра есть параметры для вывода на экран различных списков. Например, при создании профайлов отдельных пользователей для просмотра списка всех членов группы применяется опция *GRPMBR команды DSPUSRPRF. Набор списков, предусмотренных для объектов защиты, можно просмотреть с помощью приглашений команд (**F4**) и электронной информации.

Команды просмотра позволяют просматривать информацию о защите на дисплейных станциях. Дополнительные функции предоставляются также командами Работа с... (WRK). Последние выдают меню со списками. Вы можете изменять, удалять и просматривать информацию, показанную в этом меню.

Для вывода на экран и просмотра информации вы можете задавать для команд шаблоны имен. Если вы введете команду в виде `WRKUSRPRF DPT*`, то в меню Работа с регистрацией пользователей или Работа с пользовательскими профайлами будут показаны только те профайлы, имена которых начинаются на *DPT*. Параметры, для которых можно задавать шаблоны имен, перечислены в электронной справке по команде.

Изменение информации о защите

Вы можете изменять информацию о защите в интерактивном режиме с помощью команды Работа с... (WRK) или Редактировать... (EDT). Эти команды позволяют одновременно просматривать и изменять информацию.

Вы можете также изменять информацию о защите без предварительного и последующего просмотра с помощью команды Изменить... (CHG) или Предоставить... (GRT). Это способ применяется в тех случаях, когда требуется изменить сразу несколько объектов. Например, команда GRTOBJAUT применяется для задания общих прав доступа сразу ко всем объектам библиотеки (см. раздел “Задание прав доступа ко всем объектам библиотеки” на стр. 100).

Удаление информации о защите

Вы можете удалить отдельные составляющие информации о защите в интерактивном режиме с помощью команды Работа с... (WRK) или Редактировать... (EDT). Вы можете воспользоваться также командами Удалить... (DLT и RMV) и Аннулировать... (RVK). Обычно перед удалением параметров защиты система проверяет выполнение некоторых условий. В примечаниях к разделу Команды защиты перечислены некоторые из этих условий.

Добавление пользователя в систему

Для добавления нового пользователя в систему выполните следующие действия:

1. Выберите группу для этого пользователя. См. форму Описание группы пользователей.
2. Определите, будет ли этот пользователь выполнять системные функции. Если да, то укажите это в форме Полномочия в системе.
3. Добавьте информацию о пользователе в форму Профайл пользователя.
4. Просмотрев формы Полномочия в системе и Описание группы пользователей, определите, нужно ли для нового пользователя задать иные значения, нежели для остальных пользователей из этой группы.
5. Создайте профайл для нового пользователя, скопировав профайл группы или профайл существующего члена этой группы. Обязательно задайте истечение срока действия пароля. (См. раздел ″Копирование профайла группы″.)
6. Дайте новому пользователю копию бланка с информацией о конфигурации защиты.

Процедура добавления группы описана в разделе ″Создание новой группы пользователей″.

Создание новой группы пользователей

Причины, по которым может потребоваться создать новую группу пользователей, могут быть разными:

- К работе с системой подключились дополнительные отделы фирмы.
- Для повышения надежности защиты ресурсов необходимо выделить особую группу пользователей.
- Ваша фирма реорганизовала некоторые отделы.

Для создания новой группы пользователей выполните следующие действия:

1. Укажите в форме Описание группы пользователей необходимую информацию, следуя инструкциям из раздела ″Планирование групп пользователей.″
2. Добавьте группу пользователей в схему приложений, библиотек и групп.
3. Определите, будет ли кто-нибудь из группы пользователей выполнять системные функции. Обновите форму Полномочия в системе. (См. раздел ″Определение пользователей, ответственных за выполнение системных функций.″)
4. Для заполнения формы Профайл пользователя потребуется информация из форм Описание группы пользователей и Полномочия в системе.
5. Создайте библиотеку группы.
6. Создайте описание задания для группы.
7. Создайте профайл группы.

   Примечание: Инструкции по выполнению этапов 5, 6 и 7 приведены в разделе ″Настройка групп пользователей″.
8. Создайте отдельные профайлы для членов группы. (См. раздел ″Настройка профайлов пользователей.″)
9. Заполните формы Описание библиотеки для всех приложений, необходимых группе. Выполните все необходимые действия по присвоению группе доступа к объектам приложений (см. раздел ″Настройка защиты ресурсов″).
10. Раздайте всем пользователям из группы копии бланка с информацией о конфигурации защиты.

Процедура изменения параметров группы описана в разделе ″Изменение группы пользователей″.

Изменение группы пользователей

Изменение параметров группы выполняется по-разному, в зависимости от конкретного случая. Ниже приведены некоторые примеры изменений и способы их выполнения:

Изменение прав доступа группы

Пользователям группы могут потребоваться права доступа к объектам, не запланированным вами изначально. Выполните следующие действия:

1. Вызовите команду Редактировать права доступа к объекту (EDTOBJAUT) для предоставления группе требуемых прав доступа к объекту или для назначения соответствующего списка прав доступа. Пример такой процедуры приведен в разделе “Задание особых прав доступа” на стр. 104. Права доступа к объекту, предоставляемые всей группе, присваиваются каждому пользователю из этой группы.
2. Если вы предоставили некоторой группе права доступа к конфиденциальному ресурсу, рекомендуется проверить текущий состав этой группы. Для просмотра списка членов группы вызовите команду Показать пользовательский профайл (DSPUSRPRF *имя_профайла_группы* *GRPMBR).

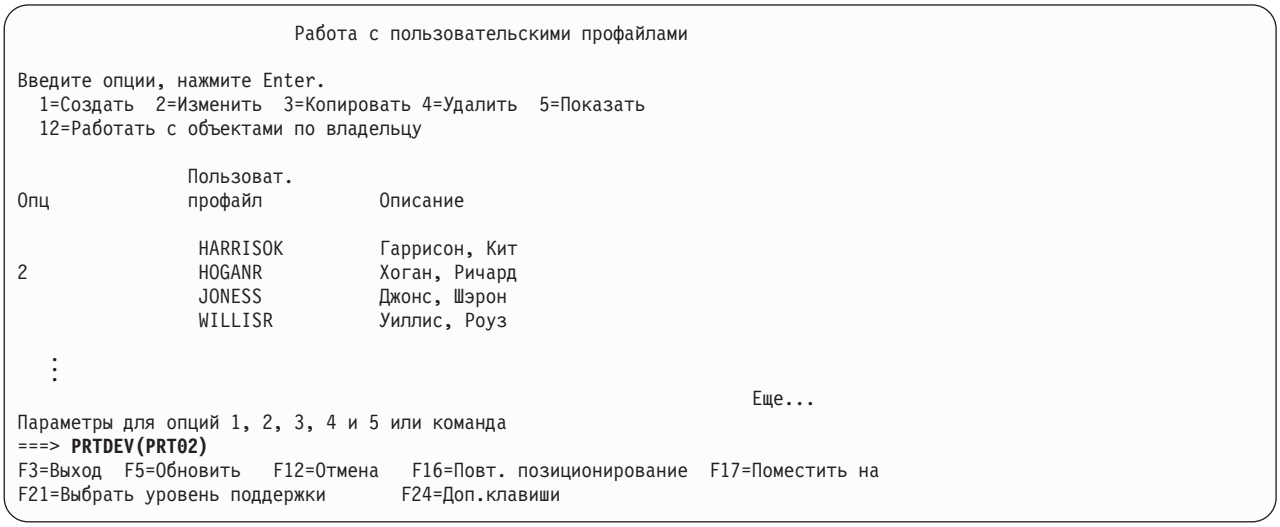
Изменение конфигурации для группы

В некоторых случаях может потребоваться изменить конфигурацию пользовательской среды для членов группы. Например, если в отделе фирмы появился отдельный принтер, то вы можете сделать его принтером по умолчанию для сотрудников этого отдела, объединенных в группу. Или, если в системе установлено новое приложение, то для пользователей группы можно задать другое начальное меню, появляющееся при входе в систему.

Вы можете использовать профайл группы в качестве шаблона, создавая профайлы членов группы путем его копирования. Последующая настройка профайла группы не повлияет на уже созданные пользовательские профайлы. Например, если вы измените значение поля *Принтер* в профайле группы, то в профайлах членов групп оно останется прежним, и в каждом из них его придется изменить отдельно.

Меню Работа с пользовательскими профайлами позволяет изменять параметры сразу в нескольких отдельных профайлах. В приведенном ниже примере показано, как изменить очередь вывода для всех элементов группы:

1. Введите WRKUSRPRF *ALL и нажмите клавишу **Enter**.
2. Если появится меню Работа с регистрацией пользователей, нажмите клавишу **F21** (Выбрать уровень поддержки) и перейдите в меню Работа с пользовательскими профайлами.



3. Укажите **2** (Изменить) рядом с именами всех профайлов, которые вы хотите изменить.
4. В строке для ввода параметров в нижней части меню введите имя параметра и его новое значение. Если вы не знаете имя параметра, нажмите **F4** (Приглашение).
5. Нажмите клавишу **Enter**. Появится подтверждающее сообщение для каждого измененного профайла.

   Хотя изменение значения в профайле группы не влияет на существующие профайлы отдельных пользователей, оно будет учтено при создании новых профайлов на его основе. Кроме того, профайл группы содержит стандартные значения для группы.

Предоставление группе прав доступа к новому приложению

Для того чтобы присвоить группе права доступа к новому приложению, необходимо проанализировать информацию о группе и о приложении. Рекомендуется следующий способ:

1. С помощью формы Описание приложения для нового приложения и схемы приложений, библиотек и групп пользователей определите, какие библиотеки используются этим приложением. Добавьте эти библиотеки в форму Описание группы.
2. Обновите схему приложений, библиотек и групп пользователей, чтобы отобразить новую взаимосвязь между группой и приложением.
3. Если эти библиотеки должны входить в начальный список библиотек для группы, измените описание задания группы с помощью команды Изменить описание задания (CHGJOBD). Если вам потребуется вспомогательная информация для работы с описаниями задания, обратитесь к разделу “Создание описания задания” на стр. 87.

   Примечание: При добавлении библиотек в начальный список библиотек в описании задания изменять пользовательские профайлы, использующие это описание, не требуется. Эти библиотеки будут добавлены в начальный список библиотек пользовательского профайла автоматически при следующем входе в систему.
4. Определите, нужно ли для назначения прав доступа к новому приложению изменить начальную программу или начальное меню. Если да, то изменения нужно будет ввести для каждого пользовательского профайла отдельно с помощью команды CHGUSRPRF.
5. Просмотрите формы Описание библиотеки для всех библиотек, используемых приложением. Проверьте, достаточно ли группе предоставленных ей общих прав доступа к библиотекам. Если нет, предоставьте группе необходимые права доступа к библиотеке, к отдельным объектам или к спискам прав доступа. Для этого воспользуйтесь командами Редактировать права доступа к объекту (EDTOBJAUT) и Редактировать список прав доступа (EDTAUTL). (Дополнительная информация приведена в разделе ″Настройка защиты ресурсов″.)

Процедуры добавления приложения в систему описаны в разделе ″Добавление нового приложения″.

Добавление нового приложения

Планирование защиты для новых приложений следует выполнять так же тщательно, как и для существующих приложений. Выполните следующие процедуры:

1. Подготовьте для добавляемого приложения формы Описание приложения и Описание библиотеки.
2. Обновите схему приложений, библиотек и групп пользователей.
3. Выполнив процедуры, описанные в разделе ″Планирование защиты ресурсов, выберите параметры защиты нового приложения.
4. Подготовьте форму Установка приложения, следуя инструкциям из раздела ″Планирование установки приложения.″
5. Определите, будет ли вывод на принтер, создаваемый этим приложением, конфиденциальным и потребуется ли установить для него защиту. При необходимости обновите форму Очередь вывода и защита рабочей станции.
6. Для установки приложения и настройки его защиты выполните действия, описанные в разделах ″Настройка принадлежности и общих прав доступа″ и ″Настройка защиты ресурсов″.

Процедуры добавления рабочей станции в систему описаны в разделе ″Добавление новой рабочей станции″.

Добавление новой рабочей станции

При добавлении новой рабочей станции в систему проверьте соблюдение следующих требований к защите:

1. Не снижает ли местонахождение рабочей станции надежность ее защиты? (См. раздел ″Планирование физической защиты″).
2. Если да, то обновите форму Очередь вывода и защита рабочей станции.
3. Обычно при создании рабочей станции ей предоставляются общие права доступа *CHANGE. Если это противоречит вашим требованиям к защите рабочей станции, вызовите команду EDTOBJAUT и укажите другие права доступа.

Информация о том, как изменить полномочия пользователя в системе, приведена в разделе ″Изменение полномочий пользователя.″

Изменение полномочий пользователя

При изменении обязанностей или полномочий пользователя необходимо отразить эти изменения в его профайле.

1. Нужно ли переместить пользователя в другую группу? Если да, то вы можете воспользоваться командой CHGUSRPRF.
2. Нужно ли изменить какие-либо значения профайла, например, принтер или начальное меню? Если да, то вы также можете воспользоваться командой CHGUSRPRF.
3. Достаточно ли пользователю частных прав доступа или прав доступа его группы к приложениям?
   - Вы можете просмотреть права доступа профайла прежней и новой групп пользователя с помощью команды Показать пользовательский профайл (DSPUSRPRF).
   - Проверьте также права доступа, заданные в профайле пользователя.
   - Внесите все необходимые изменения с помощью команды EDTOBJAUT.
4. Является ли данный пользователь владельцем каких-либо объектов? Требуется ли изменить принадлежность этих объектов? Если да, то примените команду Работа владельца с объектами (WRKOBJOWN).
5. Выполняет ли этот пользователь системные функции? Потребуется ли этому пользователю выполнять системные функции после изменения его полномочий? При необходимости обновите форму Полномочия в системе и измените параметры пользовательского профайла.

Процедуры удаления пользователя из системы описаны в разделе ″Удаление пользователя из системы″.

Удаление пользователя из системы

При уходе сотрудника из фирмы необходимо немедленно удалить его пользовательский профайл из системы. Перед удалением профайла необходимо удалить принадлежащие ему объекты или изменить их принадлежность. Для этого служит команда WRKOBJOWN или опция **4** (Удалить) меню Работа с регистрацией пользователей.

При выборе опции **4** (Удалить) для профайла в меню Работа с регистрацией пользователей появятся дополнительные меню для управления объектами, принадлежащими пользователю. Вы можете передать новому пользователю сразу все объекты или некоторые объекты по выбору:

```
                              Удалить пользователя

Пользователь . . . . . :   HOGANR
Описание пользователя. . . :   Отдел сбыта

Для удаления этого пользователя введите ниже вариант и нажмите Enter.

    1. Передать все объекты данного пользователя новому владельцу.
    2. Удалить или изменить владельца заданных объектов этого пользователя.
```

Если вы решили изменять принадлежность объектов по отдельности (опция **2**), на экране появится список всех объектов, принадлежащих пользователю:

```
                              Удалить пользователя

Пользователь . . . . . :   HOGANR
Описание пользователя. . . :   Отдел сбыта

Новый владелец . . . . . .                    Имя, F4 для списка

Для удаления этого пользователя удалите все его объекты или укажите
для них нового владельца.
Ниже введите опции и нажмите Enter.
  2=Заменить на нового владельца    4=Удалить  5=Показать сведения

Опц  Объект        Библиотека    Описание
 4   HOGANR        QUSRSYS       Очередь сообщений Ричарда Хогана
 4   QUERY1        DPTWH         Запрос данных об оборудовании
```

Если вы выбрали удаление объектов, появится меню Подтвердить удаление. После удаления объектов можно будет удалить и сам профайл. После этого вновь появится меню Работа с регистрацией пользователей с сообщением о том, что пользователь удален.

Сохранение информации о защите

В этом разделе приведен обзор процедур сохранения и восстановления информации о защите. При резервном копировании и восстановлении необходимо учитывать вопросы сохранности не только самих данных, но и информации об их защите. Перед разработкой всестороннего плана резервного копирования и восстановления ознакомьтесь с разделом Information Center Резервное копирование, восстановление и готовность системы.

Резервное копирование и восстановление информации о защите, создаваемой при настройке защиты, описывается в следующих разделах:

- Сохранение системных значений.
- Сохранение профайлов пользователей и групп.
- Сохранение описаний заданий.
- Сохранение информации о защите ресурсов.
- Применение профайла владельца по умолчанию (QDFTOWN).
- Восстановление поврежденного списка прав доступа.

Сохранение системных значений

Системные значения хранятся в системной библиотеке QSYS. Библиотека QSYS сохраняется в тех случаях, когда вы выполняете следующие операции:

- Используете команду Сохранить систему (SAVSYS).
- Используете опцию сохранения всей системы в меню Сохранить.

- Используете опцию сохранения системной информации в меню Сохранить.
- Используете опцию резервного копирования всей системы в меню Выполнить резервное копирование (RUNBCKUP).

При восстановлении всей системы из резервной копии системные значения восстанавливаются автоматически.

Перейдите к следующему разделу - Сохранение профайлов пользователей и групп.

Сохранение профайлов пользователей и групп

Профайлы пользователей и групп хранятся в библиотеке QSYS. Они сохраняются при выполнении команды Сохранить систему (SAVSYS), а также при выборе опции сохранения всей системы в меню Сохранить.

Для сохранения профайлов пользователей и групп можно также воспользоваться командой Сохранить данные защиты (SAVSECDTA).

Для восстановления пользовательских профайлов применяется команда Восстановить пользовательские профайлы (RSTUSRPRF). Ниже приведена стандартная последовательность операций при восстановлении системы:

1. Восстановить операционную систему (при этом будет восстановлена библиотека QSYS).
2. Восстановить пользовательские профайлы.
3. Восстановить остальные библиотеки.
4. Восстановить права доступа к объектам с помощью команды Восстановить права доступа (RSTAUT).

Перейдите к следующему разделу - ″Сохранение описаний заданий″.

Сохранение описаний заданий

При создании описания задания указывается библиотека, в котором будет расположено это описание. Фирма IBM рекомендует создавать описания заданий в библиотеке QGPL.

Сохранить описания заданий можно путем сохранения библиотек, в которых они расположены. Для этого применяется команда Сохранить библиотеку (SAVLIB). Кроме того, сохранить описание задания можно с помощью команды Сохранить объект (SAVOBJ).

Для восстановления содержимого библиотеки применяется команда Восстановить библиотеку (RSTLIB). Для восстановления отдельного описания задания можно воспользоваться командой Восстановить объект (RSTOBJ).

Перейдите к следующему разделу - ″Сохранение информации о защите ресурсов″.

Сохранение информации о защите ресурсов

В системе защиты ресурсов, управляющей доступом пользователей к объектам, используется информация различных типов, которая хранится в нескольких местах:

Таблица 64. Сохранение и восстановление информации, связанной с защитой ресурсов

Тип информации	Место хранения	Способ сохранения	Способ восстановления
Общие права доступа	Вместе с объектом	Команда SAVxxx [1]	Команда RSTxxx [2]
Значение контроля объекта	Вместе с объектом	Команда SAVxxx [1]	Команда RSTxxx [2]
Принадлежность объекта	Вместе с объектом	Команда SAVxxx [1]	Команда RSTxxx [2]
Основная группа	Вместе с объектом	Команда SAVxxx [1]	Команда RSTxxx [2]
Список прав доступа	Библиотека QSYS	SAVSYS или SAVSECDTA	RSTUSRPRF USRPRF(*ALL)

Таблица 64. Сохранение и восстановление информации, связанной с защитой ресурсов (продолжение)

Тип информации	Место хранения	Способ сохранения	Способ восстановления
Связь между объектом и списком прав доступа	Вместе с объектом	Команда SAVxxx [1]	Команда RSTxxx [2]
Частные права доступа	В пользовательском профайле	SAVSYS или SAVSECDTA	RSTAUT

1. Большинство объектов можно сохранить с помощью команд SAVOBJ и SAVLIB. Однако для некоторых типов объектов, таких как объекты конфигурации, существуют специальные команды сохранения.
2. Восстановить большинство объектов можно с помощью команд RSTOBJ и RSTLIB. Однако для некоторых типов объектов, таких как объекты конфигурации, существуют специальные команды восстановления.

Когда требуется восстановить приложение или всю систему, необходимо аккуратно запланировать все этапы работы, включая восстановление прав доступа к объектам. Ниже перечислены основные этапы восстановления информации о защите ресурсов приложения:

1. Если требуется, восстановите пользовательские профайлы, включая профайл-владелец приложения. Для восстановления профайлов можно воспользоваться командой RSTUSRPRF.
2. Восстановите списки прав доступа, используемые приложением. Списки прав доступа восстанавливаются при запуске команды RSTUSRPRF USRPRF(*ALL).

   Примечание: Эта команда восстанавливает из резервной копии все параметры пользовательских профайлов, включая пароли.
3. Восстановите библиотеки приложения с помощью команды RSTLIB или RSTOBJ. При этом будет восстановлена информация о принадлежности объектов, общих правах доступа и связи объектов со списками прав доступа.
4. Восстановите частные права доступа к объектам с помощью команды RSTAUT. Команда RSTAUT также восстанавливает пользовательские права доступа к спискам прав доступа. Вы можете восстановить права доступа для всех пользователей или только для отдельных профайлов.

Инструкции по восстановлению объекта и профайла владельца в другой системе приведены в разделе ″Применение профайла владельца по умолчанию (QDFTOWN)″.

Применение профайла владельца по умолчанию (QDFTOWN)

Если при восстановлении объекта профайл его владельца в системе отсутствует, то система делает владельцем восстанавливаемого объекта профайл по умолчанию - QDFTOWN. После восстановления или создания профайла владельца принадлежность объекта можно изменить с помощью команды Работа владельца с объектами (WRKOBJOWN).

Информация о восстановлении списков прав доступа приведена в разделе ″Восстановление поврежденного списка прав доступа.″

Восстановление поврежденного списка прав доступа

Если объект защищен с помощью списка прав доступа и этот список будет случайно поврежден, то доступ к объекту сохранят только пользователи, обладающих специальными правами доступа ко всем объектам (*ALLOBJ).

Восстановление поврежденного списка прав доступа состоит из двух этапов:

1. Восстановление пользователей и их прав, указанных в списке прав доступа.
2. Восстановление связи списка прав доступа с объектами.

Для выполнения этих операций требуются специальные права доступа *ALLOBJ.

Этап 1: Восстановление списка прав доступа

Если вам известны все пользователи, права которых определяются списком прав доступа, то удалите список, создайте заново и добавьте в него пользователей.

Если у вас нет информации об этих пользователях, то восстановите список прав доступа из последней резервной копии, созданной командой SAVSYS или SAVSECDTA. Для этого выполните следующие действия:

1. Удалите поврежденный список прав доступа:
   ```
   DLTAUTL AUTL(имя-списка-прав-доступа)
   ```
2. Восстановите список прав доступа:
   ```
   RSTUSRPRF USRPRF(*ALL)
   ```
3. Добавьте пользователей в список прав доступа с помощью команды Восстановить права доступа (RSTAUT).

Этап 2: Восстановление связи объектов со списком прав доступа

После того, как вы восстановили список прав доступа или создали его заново, необходимо создать связь между списком и защищаемыми объектами:

1. Воспользуйтесь командой Восстановить память (RCLSTG). Команда RCLSTG связывает объекты, которые были защищены поврежденным или утерянным списком прав доступа, со списком прав доступа по умолчанию QRCLAUTL.
2. Получите список объектов, защищенных списком прав доступа QRCLAUTL:
   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```
3. С помощью команды GRTOBJAUT свяжите эти объекты с соответствующими списками прав доступа. Например, для защиты файла ARWRK01 в библиотеке CUSTLIB с помощью списка прав доступа ARLST01, введите:
   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

Контроль защиты

В этом разделе приведены основные рекомендации по контролю за эффективностью защиты системы.

Регулярное наблюдение за работой системы защиты имеет две основные цели:

- Обеспечение адекватной защиты ресурсов компании.
- Обнаружение попыток несанкционированного доступа к системе и информации компании.

Просмотрите описание принятой стратегии защиты и разработанные для пользователей правила защиты и определите круг задач по контролю за системой защиты.

Дополнительная информация о контроле приведена в следующих разделах:

- Справочная таблица по контролю защиты.
- Контроль за действиями в системе.

Справочная таблица по контролю защиты

Ниже приведены справочные таблице для контроля различных аспектов защиты системы. Они помогут вам разработать план контроля.

Контроль физической защиты

- Обеспечьте защиту носителей с резервными копиями от повреждения и кражи.

- Ограничьте доступ к рабочим станциям в общедоступных местах. С помощью команды DSPOBJAUT определите, у каких пользователей есть права доступа *CHANGE к рабочим станциям.

Контроль системных значений

- Убедитесь в том, что параметры совпадают с указанными в форме Системные значения. Для этого воспользуйтесь командой Печать системных атрибутов защиты (PRTSYSSECA).
- Периодически анализируйте настройку системных значений, особенно при установке новых приложений.

Контроль профайлов групп

- Убедитесь, что в профайлах групп не заданы пароли. Введите команду DSPAUTUSR и убедитесь, что в качестве паролей в профайлах групп указано значение *NONE.
- Убедитесь в том, что члены групп указаны правильно. Для того чтобы получить список пользователей группы, введите команду DSPUSRPRF с опцией *GRPMBR.
- Проверьте специальные права доступа профайлов групп. Воспользуйтесь Используйтесь командой DSPUSRPRF. Если установлен уровень защиты 30, 40 или 50, у профайлов групп должны быть специальные права доступа *ALLOBJ.

Контроль пользовательских профайлов

- Убедитесь в том, что все пользовательские профайлы в системе относятся к одной из следующих категорий:
  - Профайлы работающих сотрудников
  - Профайлы групп
  - Профайлы владельцев приложений
  - Профайлы, поставляемые фирмой IBM (начинаются с буквы Q)
- Обязательно удаляйте пользовательские профайлы при увольнении пользователей или их переходе на другую работу. Для автоматического отключения или удаления профайла при увольнении пользователя используйте команду Изменить запись автоматической ликвидации профайла (CHGEXPSCDE).
- Найдите неактивные профайлы и удалите их. Для автоматического отключения профайла по истечении заданного периода бездействия вы можете воспользоваться командой Анализировать работу профайлов (ANZPRFACT).
- Определите, в каких профайлах пароли совпадают с именами пользователей. Для этого воспользуйтесь командой Анализировать пароли по умолчанию (ANZDFTPWD). Укажите в этой команду опцию, требующую замены пароля при очередном входе в систему.

  Внимание: Не удаляйте из системы профайлы, поставляемые фирмой IBM. Название таких профайлов начинается с буквы Q.
- Определите, какие пользователи не относятся к классу *USER и почему. Для просмотра списка пользователей, их классов и специальных прав доступа воспользуйтесь командой Печать пользовательских профайлов (PRTUSRPRF). Сравните полученные данные с формой Ответственные за работу системы.
- Кроме этого, обратите внимание на профайлы, у которых параметру *Ограничение возможностей* присвоено значение *NO.

Контроль важных объектов

- Определите, у кого есть доступ к важным объектам. Для контроля за этими объектами предназначены команды Печать частных прав доступа (PRTPVTAUT) и Печать объектов с общим доступом (PRTPUBAUT). Если доступ предоставлен группе, просмотрите список членов группы с помощью команды DSPUSRPRF с опцией *GRPMBR.
- Проверьте, кто может работать с программами, применяющими особые механизмы защиты, такие как принятые права доступа. Воспользуйтесь командой Печать принимающих права объектов (PRTADPOBJ).

Контроль несанкционированного доступа

- Дайте указание системным операторам обращать особое внимание на сообщения системы защиты в очереди сообщений QSYSOPR. При повторении неудачных попыток входа в систему они должны связываться с системным администратором. Идентификаторы сообщений системы защиты лежат в диапазоне от 2200 до 22FF и от 4A00 до 4AFF. Их префиксом может быть CPF, CPI, CPC или CPD.
- Настройте в системе контроль действий, обеспечивающий регистрацию попыток несанкционированного доступа к объектам.

Перейдите к следующему разделу - Контроль действий в системе.

Контроль за действиями в системе

Операционная система контролирует защиту и может заносить данные обо всех событиях, связанных с защитой, в специальные системные объекты - **получатели журнала**. Можно настроить получатели журнала для различных типов событий, связанных с защитой, таких как изменение системного значения или профайла пользователя, или безуспешная попытка доступа к объекту. Ниже перечислены значения, определяющие, какие именно события следует заносить в журнал:

- Системное значение Контроль за действиями в системе (QAUDCTL)
- Системное значение Уровень контроля за действиями в системе (QAUDLVL)
- Значение Уровень контроля за действиями в системе (AUDLVL) в профайлах пользователей
- Значение Контроля за объектами (OBJAUD) в профайлах пользователей
- Значение Контроль за объектами (OBJAUD) в объектах.

Информация из журналов контроля используется в следующих целях:

- Отслеживание попыток нарушения защиты.
- Планирование перехода на более высокий уровень защиты.
- Контроль за использованием секретных объектов (например, файлов с конфиденциальной информацией).

Для просмотра содержимого журналов контроля предусмотрены соответствующие команды.

Формы для планирования основных параметров защиты

Вы можете скопировать или распечатать эти формы из браузера.

Для того чтобы напечатать основную информацию о защите, перейдите на правую панель и щелкните на значке PDF, расположенном на вставке Information Center.

Для того чтобы напечатать конкретную форму планирования, щелкните на соответствующей ссылке. Перейдите на правую панель, а затем щелкните на значке Печать в вашем браузере. Выбранная вами форма будет напечатана.

Ниже перечислены все формы, которые требуются для успешного планирования и работы с основными параметрами защиты системы:

- Форма Планирование физической защиты
- Форма Описание приложения
- Форма Соглашения о присвоении имен
- Форма Описание библиотеки
- Форма Выбор системных значений
- Форма Полномочия в системе
- Форма Идентификация группы пользователей
- Форма Описание группы пользователей
- Форма Профайл пользователя
- Форма Список прав доступа

- Форма Защита очереди вывода и рабочей станции
- Форма Установка приложения

Форма План физической защиты

Таблица 65. План физической защиты

План физической защиты	
Составлено:	Дата:
Инструкции: • Эта форма описана в разделе ″Планирование защиты ресурсов.″ • Перечислите в форме аспекты защиты, относящиеся к физическому расположению системного блока и сопутствующих устройств. • Информацию из этой формы не требуется вводить в систему.	
Системный блок:	
Опишите меры защиты системного блока (например, запертая комната):	
Какое положение переключателя режима обычно используется?	
Где хранится ключ?	
Другие сведения о системном блоке:	
Носители резервных копий и документация:	
Где хранятся магнитные ленты с резервными копиями в офисе?	
Где хранятся магнитные ленты с резервными копиями вне вашего офиса?	
Где хранятся пароли администратора, SST и DST?	
Где хранится важная системная документация, такая как серийные номера и информация о конфигурации?	

План физической защиты			Часть 2 из 2
Дополнительные инструкции для части 2 • Перечислите все рабочие станции и принтеры, расположение которых может представлять угрозу для безопасности системы. Укажите, какие меры по защите этих устройств вы предпримете. Для принтеров укажите в столбце *Надежность защиты* примеры конфиденциальных отчетов. • Если в системе включена автоматическая настройка локальных устройств, вы можете не знать имен рабочих станций и принтеров до завершения установки системы. Если на момент заполнения формы имена неизвестны, укажите описания устройств (например, их расположение) и добавьте имена позже.			
Физическая защита принтеров и рабочих станций			
Имя рабочей станции или принтера	Расположение или описание	Надежность защиты	Необходимые меры по защите

Форма Описание приложения

Таблица 66. Описание приложения

Описание приложения	
Составлено:	Дата:
Инструкции: • Эта форма описана в разделах ″Описание приложения″ и ″Планирование защиты ресурсов.″ • Заполните отдельную форму для каждого приложения. • Информацию из этой формы не требуется вводить в систему.	
Имя приложения:	Аббревиатура:
Краткое описание приложения:	
Имя главного меню:	Библиотека:
Имя начальной программы:	Библиотека:
Перечислите библиотеки, используемые приложением для хранения файлов и программ:	
Определите требования по защите приложения, например, уровень конфиденциальности информации:	

Форма Соглашения о присвоении имен

Таблица 67. Форма Соглашение о присвоении имен

Форма Соглашение о присвоении имен	
Составлено:	Дата:
Инструкции: • Эта форма описана в разделе ″Описание приложения″. • Информацию из этой формы не требуется вводить в систему. • Опишите в этой форме правила присвоения имен системным объектам. Приведите примеры для каждого правила.	
Тип объекта	**Соглашение о присвоении имен**
Профайлы групп	
Пользовательские профайлы	
Списки прав доступа	
Библиотеки	
Файлы	
Календари	
Устройства	
Магнитные ленты	

Описание библиотеки

Таблица 68. Форма Описание библиотеки

Форма Описание библиотеки	Часть 1 из 2
Составлено:	Дата:

Таблица 68. Форма Описание библиотеки (продолжение)

Инструкции: • Эта форма описана в разделах ″Планирование защиты пользователей″ и ″Планирование защиты ресурсов.″ • Укажите в этой форме описание основных библиотек и перечислите требования по их защите. • Заполните отдельную форму для каждой крупной библиотеки приложения. • Ввод данных из этой формы описан в разделе ″Настройка защиты ресурсов.″	
Имя библиотеки:	Описание:
Кратко опишите назначение библиотеки:	
Определите требования по защите библиотеки, например, уровень конфиденциальности хранящейся в ней информации:	
Общие права доступа к библиотеке:	
Общие права доступа к объектам библиотеки:	
Общие права доступа к новым объектам (CRTAUT):	
Владелец библиотеки:	

Форма Описание библиотеки				Часть 2 из 2
Составлено:			Дата:	
Имя библиотеки:				
Дополнительные инструкции для 2 части • Перечислите пользователей и объекты, требующие особых прав доступа. • Укажите тип требуемых прав доступа: *ALL, *CHANGE, *USE или *EXCLUDE.				
Перечислите особые права доступа к объектам библиотеки				
Профайл пользователя или группы	Имя объекта	Тип объекта	Требуемые права доступа	Список прав доступа

Форма Выбор системных значений

Таблица 69. Выбор системных значений

Выбор системных значений		Часть 1 из 2
Составлено:		Дата:
Инструкции: • Эта форма описана в разделе ″Планирование общего подхода.″ • Укажите в этой форме системные значения, влияющие на защиту системы, а также их планируемую настройку. • Для ввода 1 части формы используйте опцию **1** меню Установка.		
Значения из меню Изменить системные опции		
Системное значение/ сетевой атрибут	**Рекомендуемый вариант**	**Выбранный вариант**
Имя системы		

Таблица 69. Выбор системных значений (продолжение)

Разделитель даты (QDATSEP)		
Формат даты (QDATFMT)		
Разделитель времени (QTIMSEP)		
Формат присвоения имен новым устройствам (QDEVNAMING)	1 (система iSeries)	
Системный принтер (QPRTDEV)		
Уровень защиты (QSECURITY)	40	
Разрешить системным администраторам вход в систему с любой дисплейной станции (QLMTSECOFR)	N	
Сохранять информацию учета заданий о завершении вывода на принтер (QACGLVL)	N (*NONE)	

Выбор системных значений		Часть 2 из 2
Дополнительные инструкции для части 2 • Дополнительная информация о части 2 этой формы приведена в разделе ″Установка системных значений.″ • Для ввода информации из 2 части используйте команду Работа с системными значениями (WRKSYSVAL).		
Системные значения защиты		
Системное значение	**Рекомендуемый вариант**	**Выбранный вариант**
Тайм-аут бездействующих заданий (QINACTITV)	от 30 до 60	
Очередь сообщений бездействующих заданий (QINACTMSGQ)	*DSCJOB	
Ограничить число сеансов устройств (QLMTDEVSSN)	1 (YES)	
Действие при неудачной попытке входа в систему (QMAXSGNACN)	3 (отключить оба)	
Максимальное число попыток входа в систему (QMAXSIGN)	от 3 до 5	
Срок действия пароля (QPWDEXPITV)	от 30 до 60	
Максимальная длина пароля (QPWDMAXLEN)	8	
Минимальная длина пароля (QPWDMINLEN)	6	
Требовать изменения пароля (QPWDRQDDIF)	7 (6 уникальных паролей)	
Другие системные значения		
Системное значение	**Рекомендуемый вариант**	**Выбранный вариант**
Тайм-аут бездействующих заданий (QINACTITV)	300	
Примечание: Возможно, вы захотите просмотреть другие системны значения, относящиеся к защите. Полный список системных значений, относящихся относящихся к защите, а также рекомендации по их установке приведены в третьей главе книги *Security-Reference* (SC41-5302-04).		

Форма Обязанности по обслуживанию системы

Таблица 70. Полномочия в системе

Полномочия в системе			
Составлено:			Дата:
Инструкции: • Эта форма описана в разделе ″ Планирование индивидуальных пользовательских профайлов.″ • Перечислите в этой форме всех пользователей, не относящихся к классу *USER. • Скопируйте информацию из этой формы в столбец *Класс пользователя* формы Индивидуальный пользовательский профайл.			
Кто ваш системный администратор? Кто заместитель системного администратора?			
Имя профайла	Имя пользователя	Класс	Комментарии

Форма Идентификация группы пользователей

Таблица 71. Идентификация группы пользователей

Идентификация группы пользователей								
Составлено:			Дата:					
Инструкции: • Эта форма описывается в разделе ″Планирование групп пользователей.″ • Эта форма поможет идентифицировать группы пользователей со сходными требованиями по доступу к приложениям. 1. Перечислите основные приложения в верхней части формы. 2. Перечислите пользователей в левом столбце. 3. Отметьте требуемые приложения для каждого пользователя. • Информацию из этой формы не требуется вводить в систему.								
		Необходим доступ к приложениям:						
Имя пользователя	Отдел	Прило-жение:	Прило-жение:	Прило-жение:	Прило-жение:	Прило-жение:	Прило-жение:	Прило-жение:

Таблица 71. Идентификация группы пользователей (продолжение)

Примечание: • Если вы используете *упрощенную* модель защиты, пометьте требуемые приложения символом **X**. • Если используется *строгая* модель защиты, то указывайте в ячейках таблицы символы **C** (изменение) и **V** (просмотр), чтобы показать, *как именно* используются приложения.

Форма Описание группы пользователей

Таблица 72. Описание группы пользователей

Описание группы пользователей	Часть 1 из 2
Составлено:	Дата:
Инструкции для 1 части • Подготовка этой формы описана в разделе ″Планирование групп пользователей.″ • Ввод данных из этой формы описан в разделе ″Настройка защиты пользователей.″ • Заполните отдельную форму для каждой группы пользователей. • С помощью команды Создать описание задания (CRTJOBD) создайте описание задания для каждой группы. В описании задания указывается начальный список библиотек для группы.	
Имя профайла группы: Описание группы:	
Основное приложение группы: Перечислите остальные приложения, используемые группой:	
Перечислите все требуемые группе библиотеки. Отметьте (✓) все библиотеки, которые требуется включить в начальный список библиотек группы:	
Примечание: Просмотрите форму Описание приложения для каждого из приложений, перечисленных в предыдущей части, и определите, с какими библиотеками работают эти приложения.	

Описание группы пользователей	Часть 2 из 2
Дополнительные инструкции для части 2 • В следующих таблицах перечислены все поля меню Создать пользовательский профайл. Поля объединены в две группы: поля, для которых необходимо выбрать значения, и поля, для которых фирма IBM рекомендует применять значение по умолчанию. • Для ввода в систему информации из этой части формы воспользуйтесь командой Работа с пользовательскими профайлами или командой Создать пользовательский профайл (CRTUSRPRF).	
Выберите значения для следующих полей профайла группы:	

Имя поля	**Рекомендуемый вариант**	**Выбранный вариант**
Имя профайла группы (Пользователь)		
Пароль	*NONE	
Класс пользователя (Тип пользователя)	*USER	
Текущая библиотека (Библиотека по умолчанию)	*совпадает с именем профайла группы*	
Начальная программа (программа входа в систему)		
Библиотека начальной программы		
Начальное меню (первое меню)		
Библиотека начального меню		

Ограничить возможности (Ограничить использование командной строки)	*YES	
Описание (Описание пользователя)		
Описание задания	*совпадает с именем профайла группы*	
Библиотека описания задания		
Имя профайла группы (Группа пользователей)	*NONE	
Печатающее устройство (Принтер по умолчанию)		
Очередь вывода	*DEV	
Примечание: Поля перечислены в том порядке, в котором она показаны в меню Создать пользовательский профайл (при нажатии клавиши F4).		
Оставьте значения по умолчанию для следующих полей:		
Код учета ресурсов	Буферизация ввода с клавиатуры	Общие права доступа
Уровень поддержки	ИД языка	Установить срок действия пароля
Программа Attention	Ограничение на сеансы устройств	Порядок сортировки
ИД набора символов	Максимальный объем памяти	Специальные права доступа
ИД страны или региона	Очередь сообщений	Специальная среда
Показать информацию о входе в систему	Срок действия пароля	Состояние
Пароль документа	Ограничение приоритета	Пользовательские опции
Примечание: Поля в списке расположены в алфавитном порядке.		

Форма Профайл пользователя

Таблица 73. Профайл пользователя

Профайл пользователя						
Составлено:			Дата:			
Инструкции: • Эта форма описана в разделе ″Планирование пользовательских профайлов.″ • В этой форме вы можете указать информацию об отдельных пользователях системы. Заполните отдельную форму для каждой группы пользователей (пользовательского профайла). • Дополнительную информацию о пользователях указывайте в правом столбце. • Ввод данных из этой формы описан в разделе ″Настройка пользователей.″						
Имена профайлов групп:						
Владелец созданных объектов:			Права доступа группы к созданным объектам:			
Тип прав доступа группы:						
Добавьте запись для каждого члена группы:						
Профайл	Описание	Класс пользователя	Ограничение возможностей			

Таблица 73. Профайл пользователя (продолжение)

Форма Список прав доступа

Таблица 74. Форма Список прав доступа

Форма Список прав доступа					
Составлено:			Дата:		
Инструкции: • Эта форма описана в разделе ″Планирование защиты ресурсов.″ • Заполните форму для каждого списка прав доступа. • Перечислите в форме все объекты, защищаемые данным списком, а также пользователей и группы. • Ввод данных из этой формы описан в разделе ″Настройка защиты ресурсов.″					
Имя списка прав доступа:					
Описание:					
Список объектов, защищаемых этим списком					
Имя объекта	Тип объекта	Библиотека объекта	Имя объекта	Тип объекта	Библиотека объекта
Список групп и пользователей, у которых есть доступ к этому списку					
Группа или пользователь	Разрешенный тип доступа	Разрешить управление списком	Группа или пользователь	Разрешенный тип доступа	Разрешить управление списком

Форма Защита очередей вывода и рабочих станций

Таблица 75. Защита очередей вывода и рабочих станций

Защита очередей вывода и рабочих станций				
Составлено:		Дата:		
Инструкции: • Эта форма описана в разделе ″Защита вывода на принтер″. • Добавьте в эту форму запись для каждой рабочей станции или очереди вывода, требующей особой защиты. • Ввод данных из этой формы описан в разделе ″Защита рабочих станций.″				
Список параметров защищенных очередей вывода:				
Имя очереди вывода	Библиотека очереди вывода	Показывать все файлы (DSPDTA)	Права доступа для проверки (AUTCHK)	Управляется оператором (OPRCTL)
Рабочие станции системного администратора: Если администратор может входить в систему лишь с ограниченного набора рабочих станций (системное значение QLMTSECOFR = yes), то перечислите рабочие станции, доступ к которым разрешен системному администратору и пользователям с правами доступа *ALLOBJ:				
Перечислите права доступа для рабочих станций с ограничениями:				
Имя рабочей станции	Группы и пользователи, у которых есть права доступа *CHANGE			
Примечание: Для рабочих станций с ограничениями следует установить общие права доступа *EXCLUDE.				

Форма Установка приложения

Таблица 76. Установка приложения, форма

Установка приложения		Часть 1 из 2
Составлено:		Дата:
Инструкции: • Эта форма описана в разделе ″Планирование установки приложения.″ • Заполните форму для каждого приложения, которое вы планируете установить. • Используйте эту форму при планировании принадлежности и общих прав доступа к приложениям. • Ввод данных из этой формы описан в разделе ″Настройка защиты ресурсов.″		
Имя приложения:		
Описание:		
Перечислите все профайлы, которые должны быть созданы при установке приложения, и объясните их назначение:		
Имя библиотеки:		
	До установки	После установки
Владелец библиотеки		
Владелец объекта		
Общие права доступа к библиотеке		

Таблица 76. Установка приложения, форма (продолжение)

Общие права доступа к объектам		
Общие права доступа к новым объектам		
Имя библиотеки:		
	До установки	После установки
Владелец библиотеки		
Владелец объекта		
Общие права доступа к библиотеке		
Общие права доступа к объектам		
Общие права доступа к новым объектам		

Установка приложения		Часть 2 из 2
Имя библиотеки:		
	До установки	После установки
Владелец библиотеки		
Владелец объекта		
Общие права доступа к библиотеке		
Общие права доступа к объектам		
Общие права доступа к новым объектам		
Имя библиотеки:		
	До установки	После установки
Владелец библиотеки		
Владелец объекта		
Общие права доступа к библиотеке		
Общие права доступа к объектам		
Общие права доступа к новым объектам		
Имя библиотеки:		
	До установки	После установки
Владелец библиотеки		
Владелец объекта		
Общие права доступа к библиотеке		
Общие права доступа к объектам		
Общие права доступа к новым объектам		

Приложение. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

IBM могут принадлежать патенты или заявки на патенты, относящиеся к материалам этого документа. Предоставление вам настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM
Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или в письменном виде по следующему адресу:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству: INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отказ от каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому данное заявление может не действовать в вашем случае.

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью информации по данному продукту IBM и ответственность за применение этих материалов лежит на пользователе.

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM Corporation

Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

Описанная в этой информации лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM или любого другого эквивалентного соглашения.

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. IBM не выполняла тестирование этих продуктов других фирм и не может подтвердить точность заявленной информации об их производительности, совместимости и других свойствах. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Эта информация предназначена только для планирования. Она может измениться прежде, чем описанный продукт станет доступен.

В этой публикации содержатся примеры использования данных и отчетов в повседневных деловых операциях. Для максимальной наглядности они снабжены именами людей, названиями компаний, товаров и продуктов. Все эти имена вымышлены, любое возможное сходство с названиями и адресами реальных предприятий является случайным.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и/или других странах:

Application System/400
AS/400
e (эмблема)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance и WordPro являются товарными знаками International Business Machines Corporation и Lotus Development Corporation в Соединенных Штатах и/или других странах.

C-bus является товарным знаком Corollary, Inc. в США и/или других странах.

ActionMedia, LANDesk, MMX, Pentium и ProShare являются товарными знаками или зарегистрированными товарными знаками корпорации Intel в США и/или других странах.

Microsoft, Windows, Windows NT и эмблема Windows являются товарными знаками Microsoft Corporation в США и/или других странах.

SET и эмблема SET являются товарными знаками, принадлежащими SET Secure Electronic Transaction LLC.

Java, а также все товарные знаки, содержащие слово Java, являются товарными знаками Sun Microsystems, Inc. в США и/или других странах.

UNIX является зарегистрированным товарным знаком The Open Group в США и/или других странах.

Названия других компаний продуктов и услуг могут быть товарными или сервисными знаками других компаний.

Условия загрузки и печати публикаций

Разрешение на использование выбранных для загрузки публикаций предоставляется в соответствии с следующими условиями и при подтверждении вашего с ними согласия.

Личное использование: Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

Коммерческое использование: Вы можете воспроизводить, распространять и демонстрировать данные публикации в рамках своей организации при условии сохранения информации об авторских правах. Данную публикацию, а также любую ее часть запрещается воспроизводить, распространять, использовать для создания других продуктов и демонстрировать вне вашей организации, без явного согласия IBM.

На данные публикации, а также на содержащиеся в них сведения, данные, программное обеспечение и другую интеллектуальную собственность, не распространяются никакие другие разрешения, лицензии и права, как явные, так и подразумеваемые, кроме оговоренных в настоящем документе.

Фирма IBM оставляет за собой право в любой момент по своему усмотрению аннулировать предоставленные настоящим разрешением права, если сочтет, что использование этих публикаций наносит ущерб ее интересам или что указанные инструкции не соблюдаются должным образом.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта. IBM не несет ответственности за содержание этих публикаций. Публикации предоставляются на условиях ″как есть″, без предоставления каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности или применения для каких-либо конкретных целей.

Авторские права на все материалы принадлежат IBM Corporation.

Загружая или печатая публикации с этого сайта, вы тем самым подтверждаете свое согласие с приведенными условиями.

Напечатано в Дании