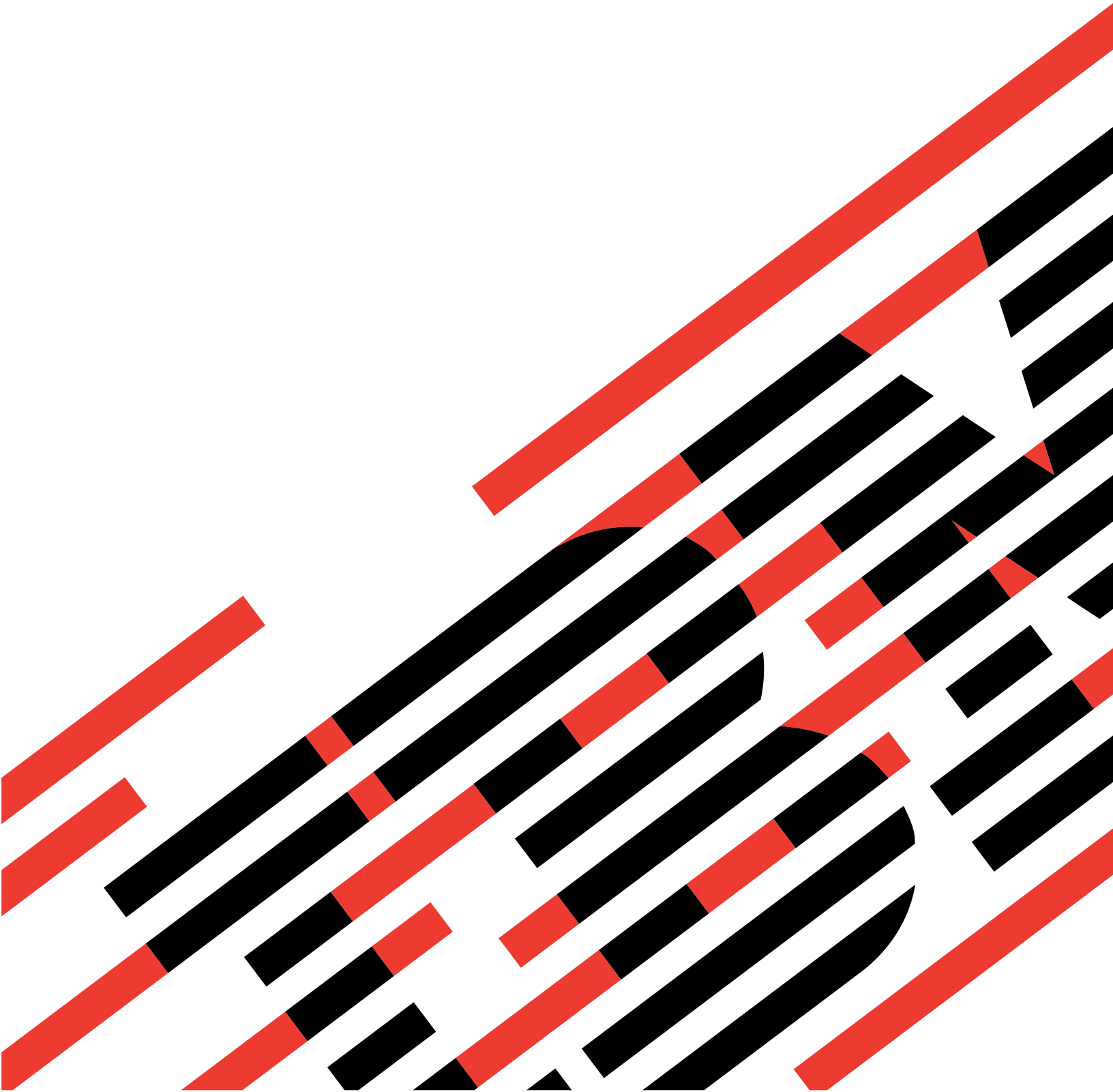
IBM

eserver

iSeries

Podstawowa ochrona systemu i jej planowanie

wersja 5 wydanie 3



IBM

@server

iSeries

Podstawowa ochrona systemu i jej planowanie

wersja 5 wydanie 3

Uwaga

Przed użyciem tych informacji oraz produktu, którego dotyczą, należy przeczytać informacje zawarte w artykule “Uwagi”, na stronie 133.

Wydanie piąte (sierpień 2005)

Niniejsze wydanie dotyczy systemu IBM Operating System/400 (numer produktu 5722-SS1) wersja 5, wydanie 3, modyfikacja 0 i wszystkich kolejnych wydań i modyfikacji, chyba że w nowych wydaniach zaznaczono inaczej. Ta wersja może pracować na wszystkich komputerach o zredukowanej liczbie instrukcji (RISC), a także na modelach CISC.

Spis treści

Podstawowa ochrona systemu i jej planowanie

Podręcznik Podstawowa ochrona systemu i jej planowanie udostępnia szczegółowe informacje dotyczące planowania i konfigurowania ochrony systemu iSeries. Ten temat kładzie nacisk na planowanie i udostępnia formularze, które można wykorzystać do planowania i zapisywania decyzji dotyczących ochrony. Udostępnia także instrukcje krok po kroku dotyczące podstawowej ochrony systemu. Z powodu ćwiczeniowej natury tego tematu, można go wydrukować, aby lepiej się z nim zapoznać.

Konfigurowanie ochrony dla systemu iSeries składa się z dwóch głównych zadań: z planowania i konfigurowania. Aby upewnić się, że skonfigurowana ochrona spełnia potrzeby przedsiębiorstwa, należy zapoznać się z poniższymi tematami dotyczącymi planowania:

- Ochrona systemu - wprowadzenie: przegląd ogólnych pojęć dotyczących ochrony oraz odpowiedzi na pytania dotyczące podstawowej ochrony systemu.
- Planowanie ochrony użytkowników: informacje na temat planowania ochrony oraz jej wpływu na użytkowników systemu. Są to między innymi planowanie ochrony fizycznej, ochrony aplikacji, ogólnej strategii ochrony oraz profili użytkowników w systemie.
- Planowanie ochrony zasobów: informacje na temat ochrony obiektów w systemie, takich jak biblioteki i zawarte w nich obiekty, drukarki, wydruki i stacje robocze.

Po wykonaniu zadań dotyczących planowania, można zapoznać się z tematami pomagającymi skonfigurować ochronę systemu:

- Konfigurowanie ochrony użytkowników: szczegóły dotyczące konfigurowania ochrony użytkowników i grup.
- Konfigurowanie ochrony zasobów: informacje na temat konfigurowania praw własności do obiektów, uprawnień publicznych i szczegółowych oraz ochrony drukarek i stacji roboczych.
- Testowanie ochrony: informacje na temat testowania ochrony.
- Zmienianie informacji o ochronie: informacje na temat aktualizowania i modyfikowania ochrony profili użytkowników, grup oraz zasobów.
- Składowanie informacji o ochronie: informacje na temat składowania informacji o ochronie.
- Monitorowanie ochrony: lista kontrolna umożliwiająca śledzenie ochrony oraz informacje na temat kontrolowania ochrony.

Oprócz tych tematów, w celu udokumentowania strategii planowania oraz decyzji dotyczących ochrony, można skorzystać z formularzy planowania.

Drukowanie tego dokumentu

W celu przeglądania i drukowania tego dokumentu można pobrać jego wersję PDF. Pliki PDF można przeglądać za pomocą programu Adobe® Acrobat® Reader. Program można pobrać ze strony głównej firmy Adobe 

Aby przejrzeć lub pobrać wersję PDF, należy wybrać Podstawowa ochrona systemu i jej planowanie (950 kB lub 164 strony).

Aby zapisać plik PDF na stacji roboczej w celu jego dalszego wykorzystania:

1. Otwórz plik PDF w przeglądarce (kliknij powyższy odsyłacz).
2. W menu przeglądarki kliknij **Plik**.
3. Kliknij **Zapisz jako...**
4. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
5. Kliknij **Zapisz**.

Ochrona systemu - wprowadzenie

Wszyscy, od administratorów systemu do użytkowników, powinni interesować się zagadnieniami dotyczącymi ochrony. Ochrona systemu zabezpiecza system iSeries oraz ważne informacje biznesowe przed zamierzonym oraz niezamierzonym naruszeniem ochrony.

Ochronę systemu można dostosować w oparciu o środowisko ochrony oraz potrzeby.

Ochronę można traktować jako wejście do systemu. Opcje ochrony wykorzystywane są do **blokowania** lub zabezpieczania informacji przed nieautoryzowanym użyciem.

Opcje ochrony można także wykorzystać do **odblokowania** elastyczności systemu i dostosowania go do każdego użytkownika.

Dobry plan ochrony może zabezpieczyć system, ale nie zagwarantuje bezpieczeństwa sprzętu lub informacji. Odpowiedzialność związaną z systemem należy podzielić między wielu pracowników tak, aby żadna osoba nie miała wyłącznej kontroli nad systemem.

Podręcznik Ochrona systemu - wprowadzenie udostępnia informacje prowadzące krok po kroku przez proces planowania i konfigurowania podstawowej ochrony systemu. Ten dokument kładzie nacisk na to, jak ważne jest planowanie ochrony systemu oraz udostępnia formularze planowania, które można wykorzystać do zapisania decyzji dotyczących ochrony. Aby pomóc w podjęciu decyzji dotyczących ochrony, zaprezentowany został przykład przedsiębiorstwa, które planuje swoją ochronę.

Aby upewnić się, że ochrona systemu będzie wystarczająca, niezbędne jest dobre i dokładne planowanie. Aby dowiedzieć się więcej na temat potrzeb ochrony oraz przekonać się, jak ważne jest jej zaplanowanie, należy zapoznać się z poniższymi tematami:

- Często zadawane pytania dotyczące podstaw ochrony systemu
- Przegląd podstawowej ochrony systemu
- Metoda planowania podstawowej ochrony systemu

Należy także przygotować dobry plan tworzenia i odtwarzania kopii zapasowych wszystkich informacji w systemie. Dodatkowo należy także zaplanować wymianę sprzętu w razie katastrofy. Więcej informacji na temat projektowania dobrego planu tworzenia kopii zapasowych, zawiera temat Składowanie i odtwarzanie w Centrum informacyjnym.

Szczegółowe informacje na temat planowania ochrony użytkowników

Przedstawione poniżej tematy udostępniają techniki dotyczące planowania ochrony użytkowników:

- Planowanie ochrony aplikacji
- Planowanie strategii ochrony
- Planowanie grup użytkowników
- Planowanie pojedynczych profili użytkowników

Szczegółowe informacje na temat planowania ochrony zasobów

Przedstawione poniżej tematy udostępniają systematyczne podejście do planowania ochrony zasobów dla użytkowników.

- Typy uprawnień
- Planowanie ochrony bibliotek aplikacji
- Określanie praw własności dla bibliotek i obiektów
- Grupowanie obiektów
- Zabezpieczanie zbiorów wydruków
- Zabezpieczanie stacji roboczych

- Planowanie instalowania aplikacji

Formularze planowania

Podręcznik Ochrona systemu - wprowadzenie udostępnia formularze planowania, które można wydrukować i w których można zapisywać wszystkie decyzje dotyczące ochrony. Można wydrukować cały dokument jako plik PDF lub pojedyncze formularze planowania, korzystając z przycisku drukowania w przeglądarce.

Instrukcje krok po kroku konfigurowania podstawowej ochrony systemu

Po zakończeniu planowania ochrony informacje zamieszczone w tym artykule ułatwią wprowadzenie tych planów w życie. Przedstawione poniżej tematy pomogą w skonfigurowaniu ochrony systemu.
- Konfigurowanie ochrony użytkowników
- Konfigurowanie ochrony zasobów

Często zadawane pytania dotyczące podstaw ochrony systemu

Zapoznanie się z odpowiedziami na często zadawane pytania dotyczące ochrony może pomóc w lepszym zrozumieniu tego, jak ważna jest ochrona systemu.

Dlaczego ochrona jest ważna?

Informacje przechowywane w systemie są jednym z najważniejszych aktywów biznesowych. Podczas zabezpieczania tych informacji należy mieć na uwadze następujące cele:
- **Poufność:** Dobre środki ochrony mogą zabezpieczyć przed oglądaniem i ujawnianiem informacji poufnych.
- **Integralność:** W niektórych obszarach dobrze zaprojektowana ochrona systemu może zapewnić większą dokładność przechowywanych danych. Za pomocą poprawnej ochrony można zabezpieczyć się przed nieautoryzowanymi zmianami lub usunięciem danych.
- **Dostępność:** Jeśli ktoś przypadkowo lub umyślnie uszkodzi dane w systemie, dostęp do tych zasobów będzie niemożliwy, do czasu ich odzyskania. Dobra ochrona systemu może zapobiec tego typu uszkodzeniom.

Kiedy ludzie myślą o ochronie systemu, zazwyczaj myślą o zabezpieczaniu swojego systemu przed osobami spoza przedsiębiorstwa, np. przed konkurencją. W rzeczywistości często największą korzyścią dobrze zaprojektowanej ochrony systemu jest zabezpieczenie przed ciekawością lub błędami popełnionymi przez właściwych użytkowników systemu. W systemie bez dobrych opcji zabezpieczających, użytkownik może usunąć ważny plik przypadkowo. Dobrze zaprojektowana ochrona systemu zabezpiecza przed tego typu wypadkami.

Przed podjęciem decyzji, jaka ochrona jest najodpowiedniejsza dla danego systemu, należy zadać sobie następujące pytania:
- Jak ważny dla przedsiębiorstwa jest dany komputer (oraz dane przechowywane na nim)?
- Czy strategia przedsiębiorstwa wymaga ustalonych poziomów ochrony?
- Czy wymagany jest pewien poziom ochrony informacji przechowywanych na danym komputerze?
- Czy w przewidywalnej przyszłości potrzebne będą pewne stopnie ochrony?

Dlaczego należy dostosowywać swój system?

System iSeries obejmuje szeroki zakres użytkowników. Mały system może mieć od trzech do pięciu użytkowników, którzy uruchamiają kilka aplikacji. Duży system może mieć tysiące użytkowników w dużej sieci komunikacyjnej, którzy uruchamiają wiele aplikacji.

Sposób, w jaki zaprojektowano system iSeries zapewnia dużą elastyczność w przystosowaniu systemu dla szerokiego zakresu użytkowników i sytuacji. Istnieje możliwość zmiany wielu parametrów dotyczących sposobu zarządzania przez system profilami użytkowników.

Po dostarczeniu systemu użytkownik prawdopodobnie nie będzie potrzebował lub nie będzie chciał go dostosowywać. Firma IBM dostarcza system z ustawieniami początkowymi, nazwanymi **domyślnymi**, dla wielu opcji. Są one zazwyczaj najbardziej odpowiednie dla nowych instalacji.

Uwaga: Wszystkie nowe systemy mają ustawiony domyślny poziom ochrony na wartość **40**. Ten poziom ochrony zapewnia, że dostęp do systemu mają tylko użytkownicy zdefiniowani. Zabezpiecza także przed potencjalnym ryzykiem naruszenia integralności lub ochrony przed programami, które mogą obejść ochronę.

Jednak dostosowanie systemu może uczynić go łatwiejszym oraz bardziej wydajnym narzędziem dla użytkowników. Na przykład można zapewnić, że użytkownik po każdym wpisaniu się zawsze będzie miał dostęp do konkretnego menu. Można zapewnić, że każdy raport użytkownika znajdzie się we właściwej drukarce. Użytkownicy poczują się pewniej w systemie, jeśli początkowe dostosowanie upodobni go do ich własnych systemów.

Kto powinien być odpowiedzialny za ochronę?

Różne przedsiębiorstwa mają różne podejście do ochrony. Niekiedy za wszystkie aspekty ochrony odpowiedzialni są programiści. W innych przypadkach osoba zarządzająca systemem odpowiada także za ochronę. Jeśli użytkownik nie jest pewny, w jaki sposób podzielić odpowiedzialność, poniżej przedstawiono kilka sugestii:

- Metoda planowania ochrony zasobów zależy od tego, czy przedsiębiorstwo kupuje, czy samo tworzy aplikacje. Jeśli aplikacje tworzone są samodzielnie, wymagania ochrony należy przekazać podczas procesu projektowania. Jeśli aplikacje są kupowane, należy współpracować z projektantem aplikacji. W obu przypadkach osoby projektujące aplikacje, jako część projektu, powinny rozważyć także ochronę.
- Konfigurowanie ochrony powinno być obowiązkiem szefa ochrony. Szef ochrony definiuje użytkowników systemu oraz ich dostęp do niego. Szef ochrony często jest odpowiedzialny za inne działania w systemie, takie jak składowanie i odtwarzanie informacji.
- Szef ochrony powinien także dostosować system, gdyż w dostosowywaniu systemu ważną rolę odgrywa wiele elementów dotyczących ochrony.

Bez względu na to, która metoda zostanie wykorzystana do przypisania odpowiedzialności za ochronę, należy **opracować strategię ochrony**. Kierownik powinien przekazać wszystkim, najlepiej na papierze, że informacje w komputerze są ważnymi aktywami. Należy je chronić, tak jak inne aktywa przedsiębiorstwa. Przykład strategii ochrony zawiera sekcja ″Przykład: strategia ochrony przedsiębiorstwa JKL Toy″.

Po zrozumieniu potrzeby ochrony systemu można zapoznać się z przeglądem uwag dotyczących ochrony systemu.

Przegląd podstawowej ochrony systemu

Aby planować efektywnie, należy zrozumieć, w jaki sposób zadania realizowane przez użytkowników są powiązane z narzędziami udostępnianymi przez system. Należy wiedzieć, w jaki sposób użytkownik i funkcje systemowe współdziałają ze sobą, co pomaga w osiągnięciu wyznaczonych celów.

Wymienione poniżej tematy przedstawiają ważne elementy dotyczące ochrony oraz konfigurowania, a także prezentują ich dopasowanie. Te tematy zawierają informacje, z którymi warto się zapoznać przed rozpoczęciem planowania. Wszystkie przedstawione tutaj pojęcia będą szczegółowo wyjaśnione w momencie, gdy będzie wymagał tego proces planowania.

- Wbudowana ochrona systemu
- Podstawowa terminologia
- Pogląd użytkownika na ochronę
- Narzędzia systemowe do ochrony i dostosowywania

Wbudowana ochrona systemu

Wszystkie elementy ochrony systemu są wbudowane w system. Nie są oddzielnym produktem, który należy kupić. Takie zintegrowane środowisko przynosi kilka korzyści:

- ochrona jest spójna z resztą systemu operacyjnego, korzysta z tych samych ekranów, komend oraz terminologii,

- użytkownicy nie mogą obejść ochrony, ponieważ nie jest oddzielnym programem,
- poprawnie zaprojektowana ochrona ma minimalny wpływ na wydajność,
- taka ochrona zawsze jest dostępna z nowymi wersjami oprogramowania; kiedy udostępniane są nowe funkcje, udostępniana jest także ochrona tych funkcji.

System iSeries dostarczany jest z poziomem ochrony 40, który zabezpiecza przed wpisywaniem się do systemu nieautoryzowanych użytkowników. Zabezpiecza także przed potencjalnym ryzykiem naruszenia integralności lub ochrony przed programami, które mogą obejść ochronę. Jednak istnieje możliwość dostosowania niektórych ustawień ochrony lub zmiany poziomów ochrony. Poziomy ochrony opisane są w temacie ″Wybieranie poziomu ochrony.″

Po zrozumieniu wbudowanych funkcji ochrony można zapoznać się z powszechnie używaną terminologią systemu iSeries .

Podstawowa terminologia

Aby zrozumieć zagadnienia ochrony systemu iSeries, bardzo ważna jest znajomość ogólnej terminologii:

Obiekt (object)
Obiekt to nazwana przestrzeń systemu, którą można manipulować. Najlepszymi przykładami obiektów są zbiory, pliki i programy. Pozostałe rodzaje obiektów to między innymi komendy, kolejki, biblioteki i foldery. Obiekt jest identyfikowany w systemie przez nazwę obiektu, rodzaj obiektu oraz bibliotekę, w której się znajduje. Każdy obiekt może być zabezpieczony.

Biblioteka (library)
Biblioteka to specjalny rodzaj obiektu, który jest wykorzystywany do grupowania innych obiektów. Wiele obiektów systemowych znajduje się w jednej bibliotece.

Katalog (directory)
Katalog to inny sposób grupowania obiektów w systemie. Obiekty mogą znajdować się w katalogu. Katalog może znajdować się w innym katalogu, tworząc strukturę hierarchiczną.

Po lepszym zrozumieniu ogólnej terminologii ochrony systemu iSeries warto się dowiedzieć, jak użytkownicy postrzegają ochronę.

Pogląd użytkownika na ochronę

Z punktu widzenia użytkownika ochrona wpływa na to, jak może on korzystać z systemu i wykonywać w nim zadania. Istnienie ochrony wpływa także na możliwość współpracy z systemem podczas wykonywania tych zadań. Dlatego ważną czynnością jest rozważenie, jak użytkownik będzie widział ochronę. Na przykład ustawienie hasła tracącego ważność co pięć dni może frustrować i przeszkadzać użytkownikowi w wykonywaniu jego zadań. Z drugiej strony, zbyt luźna strategia dotycząca hasła może spowodować problemy z ochroną.

W celu zapewnienia poprawnej ochrony systemu należy podzielić ją na określone części, które można zaplanować, zarządzać i monitorować. Z punktu widzenia użytkownika, ochronę systemu można podzielić na kilka części:

Fizyczny dostęp do systemu

Ochrona fizyczna zabezpiecza przed przypadkowym lub zamierzonym uszkodzeniem lub utratą jednostki systemowej, wszystkich urządzeń systemowych oraz nośników pamięci zawierających kopie zapasowe, takich jak dyskietki, taśmy lub dyski CD.

Większość podejmowanych środków ochrony fizycznej jest niezależnych od systemu. Jednak system dostarczany jest z blokadą lub kluczem elektronicznym, który zabezpiecza przed nieautoryzowanym użyciem funkcji jednostki systemowej.

Temat ″Planowanie ochrony fizycznej″ udostępnia szczegółowe informacje na temat planowania ochrony fizycznej systemu.

Sposób wpisywania się

Ochrona wpisywania się zabezpiecza przed wpisywaniem się osób, które nie są zidentyfikowane w systemie. Aby wpisać się do systemu, należy podać poprawną kombinację identyfikatora użytkownika i hasła.

Aby zapewnić, że ochrona wpisywania się nie zostanie naruszona, można używać zarówno wartości systemowych, jak i pojedynczych profili użytkowników. Na przykład można wymagać, aby hasła były zmieniane regularnie. Można także zapobiec używaniu łatwych do odgadnięcia haseł.

Co użytkownik może robić

Ważnym elementem ochrony oraz dostosowywania systemu jest definiowanie czynności, które mogą wykonywać użytkownicy. Z perspektywy ochrony często jest to **ograniczanie** funkcji, co na przykład uniemożliwia przeglądanie pewnych informacji. Z perspektywy dostosowywania systemu jest to **udostępnianie** funkcji. Poprawnie skonfigurowany system umożliwia użytkownikom poprawne wykonywanie zadań oraz wyeliminowanie niepotrzebnych zadań i informacji.

Niektóre metody definiowania, co użytkownik może zrobić, są przeznaczone dla szefa ochrony, inne dla programistów. Informacje w tym temacie skupiają się przede wszystkim na tych zadaniach, które zazwyczaj wykonuje szef ochrony. Opis wszystkich wartości systemowych zawiera rozdział 3, ″Wartości systemowe dotyczące ochrony″, podręcznika *Ochrona* (SC85-0124).

Do ustawiania możliwości użytkownika w systemie służą parametry pojedynczego profilu użytkownika, opisy zadań oraz klasy. Przedstawiona poniżej lista zawiera krótki opis dostępnych technik:

Ograniczanie dostępu użytkowników do kilku funkcji
: Korzytając z profilu użytkownika można umożliwić użytkownikowi dostęp tylko do określonego programu, menu lub zestawu menu oraz kilku komend systemowych. Zazwyczaj to szef ochrony tworzy profile i zarządza nimi.

Ograniczanie funkcji systemowych
: Funkcje systemowe umożliwiają składowanie i odtwarzanie informacji, zarządzanie zbiorami wydruków oraz konfigurowanie nowych użytkowników systemu. Każdy profil użytkownika określa, które z najczęściej używanych funkcji systemowych może wykonywać użytkownik.

  W systemie iSeries funkcje systemowe można wykonywać za pomocą języka komend CL i interfejsów programistycznych (API). Ponieważ każda komenda i interfejs API jest obiektem, za pomocą uprawnień do obiektu można kontrolować, kto może ich używać i wykonywać funkcje systemowe.

Określanie, kto może korzystać z plików i programów
: Ochrona zasobów udostępnia możliwość kontrolowania użycia każdego obiektu w systemie. Dla każdego obiektu można podać, kto może go używać oraz jak go używać. Na przykład można określić, że jeden użytkownik może tylko przeglądać informacje zawarte w pliku lub zbiorze, inny może je zmieniać, a jeszcze inny może zmieniać plik lub zbiór albo całkowicie go usunąć.

Zabezpieczanie przed nadużywaniem zasobów systemowych
: Moc przetwarzania systemu może stać się ważna dla przedsiębiorstwa, tak samo jak dane w nim przechowywane. Jednym z zadań szefa ochrony jest zapewnienie, aby użytkownicy nie nadużywali zasobów systemowych przez uruchamianie swoich zadań z wysokim priorytetem, drukowanie najpierw swoich raportów lub używanie zbyt dużej pamięci dyskowej.

W jaki sposób system komunikuje się z innymi systemami

Jeśli system komunikuje się z innymi komputerami lub programowalnymi stacjami roboczymi, konieczne mogą być dodatkowe środki ochrony. Jeśli w systemie nie ma odpowiedniej kontroli ochrony, użytkownik innego komputera w danej sieci może uruchomić zadanie lub uzyskać dostęp do informacji bez przechodzenia przez proces wpisywania się.

Do kontrolowania, czy możliwe jest wykonywanie zdalnych zadań, zdalny dostęp do danych lub zdalny dostęp z komputera PC, można wykorzystać zarówno wartości systemowe, jak i atrybuty sieciowe. Jeśli zdalny dostęp jest

dozwolony, można ustawić odpowiednie parametry ochrony. Opis wszystkich wartości systemowych zawiera rozdział 3, ″Wartości systemowe dotyczące ochrony″, podręcznika *Ochrona* (SC85-0124).

W jaki sposób składować informacje o ochronie

Należy regularnie wykonywać kopię zapasową informacji w systemie. Oprócz składowania danych systemu, należy składować także informacje o ochronie. W razie awarii potrzebne będzie odtworzenie informacji o użytkownikach systemu, informacji o autoryzacji oraz samych informacji.

Temat ″Składowanie informacji o ochronie″ wyjaśnia sposób składowania informacji o ochronie. Szczegółowe informacje na temat składowania i odtwarzania danych ochrony zawiera temat Składowanie i odtwarzanie w Centrum informacyjnym.

W jaki sposób monitorować plan ochrony

System udostępnia kilka narzędzi do monitorowania efektywności ochrony:

- w razie naruszenia ochrony wysyłane są komunikaty do operatora systemu,
- w specjalnej kronice kontroli mogą być zapisywane różne transakcje związane z ochroną.

W temacie ″Monitorowanie ochrony″ omówiono sposób użycia tych narzędzi. Więcej informacji na temat kontrolowania ochrony można znaleźć w rozdziale 9, ″Kontrolowanie ochrony systemu″ podręcznika *Ochrona* (SC85-0124).

Aby lepiej zrozumieć sposób konfigurowania systemu, warto spojrzeć na konfigurowanie z punktu widzenia użytkownika.

Konfigurowanie systemu z punktu widzenia użytkownika: System można tak skonfigurować, aby ułatwić użytkownikom wykonywanie codziennej pracy. Aby jak najlepiej skonfigurować system pod kątem użytkowników, należy zastanowić się, czego potrzebują do wykonywania swojej pracy. W celu dostosowania menu i aplikacji, system można skonfigurować na kilka sposobów:

Wyświetlanie użytkownikom tego, co chcą zobaczyć

Większość użytkowników tak planuje swoje biurka oraz biura, aby mieć łatwiejszy dostęp do potrzebnych rzeczy. W ten sam sposób należy myśleć o dostępie użytkowników do systemu. Po wpisaniu się do systemu użytkownik najpierw powinien zobaczyć menu lub ekran, którego najczęściej używa. W tym celu łatwo można zaprojektować profile użytkowników.

Eliminowanie niepotrzebnych elementów

W większości systemów znajduje się wiele różnych aplikacji. Natomiast większość użytkowników chce widzieć tylko elementy potrzebne im do pracy. Ograniczenie ich do kilku funkcji w systemie ułatwi im pracę. Określony widok na system można zapewnić za pomocą profili użytkowników, opisów zadań oraz odpowiednich menu.

Wysyłanie obiektów do odpowiednich miejsc

Użytkownicy nie powinni martwić się o to, jak wysyłać swoje raporty do odpowiedniej drukarki oraz jak ich zadania wsadowe powinny być uruchamiane. Za te rzeczy odpowiadają wartości systemowe, profile użytkowników oraz opisy zadań.

Udostępnianie asysty

Nieważne jak dobrze będzie skonfigurowany system, użytkownicy nadal będą zastanawiali się ″Gdzie jest mój raport?″ lub ″Czy moje zadanie zostało uruchomione?″ Ekrany **Asysty Operacyjnej** udostępniają prosty interfejs funkcji

systemowych, które pomagają użytkownikom odpowiedzieć na takie pytania. Różne wersje ekranów systemowych, nazywanych **poziomami asysty**, udostępniają pomoc dla użytkowników o różnych poziomach doświadczenia technicznego. W nowym systemie, ekrany Asysty Operacyjnej automatycznie są dostępne dla wszystkich użytkowników. Jednak projekt aplikacji może wymagać zmiany sposobu dostępu do Asysty Operacyjnej przez użytkowników.

System iSeries udostępnia narzędzia systemowe , które umożliwiają konfigurowanie ochrony systemu tak, aby zabezpieczał zasoby podczas dostępu do nich.

Narzędzia systemowe do ochrony i konfigurowania

Aby planować efektywnie, należy zrozumieć, w jaki sposób można powiązać z celami ochrony narzędzia udostępniane przez system. Narzędzia systemowe można wykorzystać podczas konfigurowania ochrony systemu.

Poziom ochrony

Firma IBM dostarcza system iSeries z ustawieniem poziomu ochrony 40. Poziom ochrony 40 udstępnia ochronę za pomocą hasła, ochronę zasobów oraz integralność systemu. Jeśli użytkownik chce zmienić aktywny poziom ochrony systemu, może zmienić wartość systemową QSECURITY. Jednak firma IBM zaleca pozostawienie poziomu ochrony 40. Aby zmienić poziom ochrony, użytkownik musi mieć klasę użytkownika *SECOFR lub uprawnienia specjalne *ALLOBJ i * SECADM.

System oferuje cztery poziomy ochrony, które zostały przedstawione w poniższej tabeli:

Tabela 1. Poziomy ochrony dostępne w systemie

Poziom ochrony	**Opis**
Poziom ochrony 20	Udostępnia tylko ochronę za pomocą hasła.
Poziom ochrony 30	Udostępnia ochronę za pomocą hasła oraz ochronę zasobów.
Poziom ochrony 40	Udostępnia ochronę za pomocą hasła, ochronę zasobów oraz ochronę integralności.
Poziom ochrony 50	Udostępnia ochronę za pomocą hasła, ochronę zasobów oraz zaawansowaną ochronę integralności.

Szczegółowe informacje na temat sposobu określania poziomu ochrony najlepiej spełniającego wymagania użytkownika, udostępnia temat ″Wybieranie poziomu ochrony ″.

Wartości systemowe

Niektórymi funkcjami systemu iSeries można sterować za pomocą wartości systemowych. Wartości systemowe można traktować jako strategię dla przedsiębiorstwa. Wartości systemowe mają wpływ na działanie każdego użytkownika systemu, chyba że zostaną zastąpione wartościami z profilu użytkownika.

Wartości systemowe określają takie elementy, jak główna drukarka, sposób wyświetlania daty oraz częstotliwość zmiany hasła.

Atrybuty sieciowe

Atrybuty sieciowe określają niektóre charakterystyki dotyczące komunikowania się systemu z innymi komputerami, także osobistymi. Atrybuty sieciowe mają zastosowanie do całego systemu.

Profile grupowe

Profile grupowe definiują grupę użytkowników. Można je traktować jako strategię dla przedsiębiorstwa. Są to również wzorce podczas tworzenia pojedynczych profili użytkowników. Można ich także używać do określania, jakiego rodzaju i do jakich obiektów systemu mają dostęp członkowie grupy. Więcej informacji na temat profili grupowych zawiera temat ″Planowanie grup użytkowników.″

Profile użytkowników

Profil użytkownika to jeden z najpotężniejszych i najbardziej uniwersalnych obiektów w systemie. Zawiera takie elementy, jak hasło użytkownika czy menu początkowe, które użytkownik widzi po wpisaniu się. Profil użytkownika definiuje, co dana osoba może lub czego nie może zrobić w systemie. Określa unikalną perspektywę widzenia systemu przez użytkownika. Omówienie wskazówek dotyczących planowania profili użytkowników zawiera temat ″Planowanie ochrony użytkowników″.

Opisy zadań

Opis zadania współpracuje z wartościami systemowymi oraz z profilami użytkowników w celu określenia sposobu przetwarzania zadań użytkownika przez system. Opis zadania konfiguruje początkową listę bibliotek użytkownika, czyli biblioteki, do których, po wpisaniu się, użytkownik uzyskuje automatyczny dostęp.

Ochrona zasobów

Szef ochrony zabezpiecza zasoby (obiekty) w systemie określając kto ma uprawnienia do korzystania z nich oraz jak może uzyskać do nich dostęp. Szef ochrony może ustawić uprawnienia do obiektu dla pojedynczych obiektów lub dla grup obiektów (listy autoryzacji). Obiektami wymagającymi zabezpieczenia są pliki, zbiory, programy i biblioteki, ale ochrona systemu umożliwia ustawienie uprawnień do obiektu dla każdego obiektu w systemie.

Jeśli zaplanowane zostanie ogólne i proste podejście, zarządzanie ochroną zasobów może być proste oraz efektywne. Schemat ochrony zasobów utworzony bez wcześniejszego planowania, może stać się skomplikowany oraz nieefektywny. W temacie ″Planowanie ochrony zasobów″ opisano sposoby planowania ochrony zasobów.

System udostępnia kilka narzędzi pomagających zaprojektować prosty schemat ochrony zasobów:

- **Profile grupowe:** podobnych użytkowników można zgrupować w jednym profilu grupowym. Dzięki temu grupa użytkowników będzie mogła współużytkować te same uprawnienia do obiektów.
- **Listy autoryzacji:** obiekty można zgrupować w listy, kierując się podobnymi wymaganiami ochrony. Następnie można nadawać uprawnienia do list, a nie do pojedynczych obiektów.
- **Prawo własności do obiektu:** każdy obiekt w systemie ma swojego właściciela. Właścicielem obiektu może być profil grupowy lub indywidualny użytkownik. Prawidłowe przypisanie prawa własności do obiektu pomaga (1) zarządzać aplikacjami oraz (2) delegować odpowiedzialność związaną z ochroną informacji.
- **Grupa podstawowa:** dla obiektu można określić uprawnienia grupy podstawowej. Uprawnienia grupy podstawowej przechowywane są razem z obiektem. Korzystanie z tej grupy może ułatwić zarządzanie uprawnieniami oraz podnieść wydajność sprawdzania uprawnień.
- **Uprawnienia do biblioteki:** pliki i programy wymagające zabezpieczeń można umieścić w konkretnej bibliotece i ograniczyć dostęp do tej biblioteki. Często jest to łatwiejsze rozwiązanie niż ograniczanie dostępu do każdego pojedynczego obiektu. Aby zabezpieczyć obiekty krytyczne, można chronić zarówno obiekt, jak i bibliotekę.
- **Uprawnienia do obiektu:** jeśli dostęp do biblioteki nie jest ograniczony, można ograniczyć uprawnienia do pojedynczych obiektów, takich jak zbiory lub pliki.
- **Uprawnienia publiczne:** dla każdego obiektu można zdefiniować, jaki rodzaj dostępu do niego ma użytkownik systemu, który nie ma żadnych innych uprawnień do obiektu. Uprawnienia publiczne to skuteczny sposób na zabezpieczanie obiektów, które nie są poufne; zapewniają one także dobrą wydajność systemu.
- **Uprawnienia do katalogu:** uprawnienia do katalogu można używać w ten sam sposób, jak uprawnienia do biblioteki. Obiekty można pogrupować w katalogi i zabezpieczać katalogi, a nie pojedyncze obiekty.

- **Magazyn uprawnień:** podczas usuwania obiektu usuwane są także informacje o uprawnieniach do tego obiektu. Magazyn uprawnień obsługuje informacje o uprawnieniach dla zbiorów definiowanych programowo, które są usuwane i ponownie tworzone przez aplikację. Magazyn uprawnień można wykorzystać jako asystę podczas migrowania z systemu System/36.

Narzędzia ochrony

Narzędzia ochrony można wykorzystywać do pomocy przy zarządzaniu i monitorowaniu środowiska ochrony w systemie iSeries. Narzędzi do obsługi profili użytkowników można użyć także do:

- sprawdzania, które profile użytkowników mają domyślne hasła,
- sporządzania harmonogramu wyłączania profili użytkowników o określonych godzinach dnia lub tygodnia,
- planowania usuwania profilu użytkownika w momencie odejścia pracownika,
- sprawdzania, które profile użytkowników mają uprawnienia specjalne,
- sprawdzania, kto adoptuje uprawnienia do obiektów w systemie.

Narzędzia do ochrony obiektów mogą być wykorzystywane do śledzenia uprawnień publicznych i prywatnych, które są związane z obiektami poufnymi. Takie raporty mogą być drukowane regularnie (na przykład co miesiąc), aby pomóc użytkownikowi skupić się na błędach ochrony dotyczących bieżących zagadnień. Kolejne raporty zawierają tylko zmiany wprowadzone od ostatniego uruchomienia raportu.

Pozostałe narzędzia dają możliwość monitorowania:

- programów wyzwalanych,
- wartości w pozycjach komunikacyjnych, opisach podsystemów, kolejkach wyjściowych, kolejkach zadań i opisach zadań, które dotyczą ochrony,
- zmodyfikowanych lub manipulowanych programów.

Po zrozumieniu, jak ważna jest ochrona systemu, można zapoznać się z opisem metody planowania, która została wykorzystana w przykładzie.

Metoda planowania podstawowej ochrony systemu

Tematy dotyczące planowania zawarte w tym dokumencie przedstawiają podejście do planowania od strony zewnętrznej do wewnętrznej oraz od ogółu do szczegółu. Na przykład podczas planowania profili użytkowników, najpierw należy zastanowić się, co użytkownik powinien widzieć (strona zewnętrzna), a następnie zdecydować, jak to zrobić (strona wewnętrzna). Najpierw należy zaplanować wartości systemowe oraz profile grupowe (ogólnie), a następnie zadecydować o wyjątkach dla pojedynczych użytkowników (szczegółowo). Kroki dotyczące planowania, które przedstawiono w temacie Planowanie ochrony użytkowników, zaprojektowano tak, aby je wykonać w podanej kolejności. Odzwierciedlają one logiczną sekwencję planowania wykorzystania systemu oraz jego dostosowania i ochrony.

Planowanie i projektowanie ochrony systemu należy rozpocząć od podstaw, od najbardziej podstawowych form ochrony, a następnie przejść do bardziej złożonych zagadnień. Należy rozpocząć od ochrony fizycznej systemu, a następnie przejść do opisywania aplikacji i wartości systemowych. Na końcu należy rozważyć ochronę użytkowników oraz obiektów w systemie.

Dla wszystkich tematów dotyczących planowania udostępnione zostały przykłady na podstawie scenariusza dotyczącego przedsiębiorstwa JKL Toys. Temat ″Przykład: prezentacja przedsiębiorstwa JKL Toy″ opisuje przykładowe przedsiębiorstwo, które zostało wykorzystane w tematach planowania.

Krótkie opisy wszystkich kroków oraz wzajemnych powiązań między nimi zawiera temat ″Kroki w procesie planowania″.

Przykład: przedstawienie przedsiębiorstwa JKL Toy

Przykłady ułatwiają wyjaśnienie oraz zrozumienie niektórych rzeczy. Pamiętając o tym, w tematach wykorzystano przykład przedsiębiorstwa JKL Toy. Przedsiębiorstwo JKL Toy, mały ale szybko rozwijający się producent zabawek,

chce skonfigurować ochronę w systemie iSeries. Prezes John Smith chce, aby nowy system iSeries zmniejszył obciążenie związane z rozrostem przedsiębiorstwa JKL Toy.

John przekazał odpowiedzialność administratora systemu oraz szefa ochrony Sharon Jones, księgowej. Chce ona mieć pewność, że cały proces instalacji, łącznie z ustawieniem ochrony, przebiegnie gładko. Sharon wie, jak ważne jest planowanie. Dziś przedsiębiorstwo jest małe, a większość pracowników ma dostęp do większości informacji. Ale Sharon wie, że ta sytuacja zmieni się, gdy przedsiębiorstwo rozrośnie się. Chce wszystko zrobić poprawnie za pierwszym razem.

Początkowo przedsiębiorstwo JKL Toy planuje uruchomić w systemie następujące aplikacje: Zamówienia klientów, Kontrola zapasów, Kontrakty i wycena oraz Należności. W miarę czytania tematów dotyczących planowania będzie można dowiedzieć się więcej na temat ochrony w przedsiębiorstwie JKL Toy.

Temat ″Kroki w procesie planowania″ wyjaśnia każdy krok, który trzeba wykonać podczas planowania ochrony systemu.

Kroki w procesie planowania ochrony

Poniższy wykres opisuje każdy krok w procesie planowania oraz jego wpływ na pozostałą część procesu.

Tabela 2. Kroki w procesie planowania ochrony

Krok	**Co należy wykonać w tym kroku**	**Jak ten krok jest powiązany z innymi krokami**
Planowanie ochrony fizycznej	Opisuje jak zaplanować zabezpieczenie jednostki systemowej, urządzeń oraz nośników składowania.	Większość tych informacji jest niezależna od reszty procesu. Informacje dotyczące planowania ochrony fizycznej nie są wprowadzane do systemu; jednak niektóre informacje są potrzebne do zaplanowania wartości systemowych oraz ochrony zasobów.
Planowanie ochrony aplikacji	Opisuje przeznaczenie, menu główne oraz biblioteki wszystkich aplikacji.	Udostępnia podstawowe informacje dla reszty procesu planowania oraz innych decyzji dotyczących ochrony. Tych informacji nie wprowadza się do systemu.
Planowanie ogólnej strategii ochrony	Należy zdecydować, jakie będzie ogólne podejście do ochrony. Należy wybrać wartości systemowe, które umożliwią realizację przyjętych założeń.	W celu określenia ogólnego podejścia, należy skorzystać z informacji planowania aplikacji. Wybrane wartości systemowe wpływają na sposób planowania profili użytkowników i grup.
Planowanie grup użytkowników	Należy zdecydować, jak podzielić użytkowników na grupy. Należy określić charakterystykę każdej grupy oraz sposób jej zdefiniowania w systemie.	W celu określenia grup w systemie należy skorzystać z opisywania aplikacji. Sposób definiowania grup użytkowników wpływa na sposób planowania pojedynczych użytkowników systemu.
Planowanie pojedynczych profili użytkowników	Każdego użytkownika systemu należy przypisać do grupy. Należy zdefiniować każdego użytkownika podając charakterystyki, które różnią go od reszty grupy. Na przykład użytkownik wymaga dostępu do aplikacji lub biblioteki innej niż reszta grupy.	W celu zdefiniowania pojedynczych użytkowników, należy wykorzystać informacje dotyczące planowania aplikacji oraz grup użytkowników.
Planowanie ochrony zasobów	Należy zdecydować, które aplikacje mają być dostępne dla każdego użytkownika w systemie. Jeśli użycie pewnych aplikacji ma być ograniczone, należy zdecydować, którzy użytkownicy oraz które grupy mają mieć do nich dostęp.	W celu zaplanowania ochrony zasobów należy wykorzystać informacje dotyczące planowania aplikacji oraz profili grupowych.

Tabela 2. Kroki w procesie planowania ochrony (kontynuacja)

Krok	Co należy wykonać w tym kroku	Jak ten krok jest powiązany z innymi krokami
Planowanie instalowania aplikacji	Należy zdecydować, w jaki sposób ustanowić prawo własności oraz uprawnienia publiczne dla bibliotek aplikacji.	Podczas planowania instalowania aplikacji należy wykorzystać informacje planowania ochrony zasobów.

Proces planowania ochrony należy rozpocząć od planowania ochrony użytkowników.

Planowanie ochrony użytkowników

Planowanie ochrony użytkowników obejmuje planowanie wszystkich obszarów, w których ochrona wpływa na użytkowników systemu. Istotne jest opisanie następujących obszarów:

Ochrona fizyczna
Ochrona fizyczna obejmuje zabezpieczenie systemu iSeries przed przypadkowym (lub zamierzonym) uszkodzeniem lub kradzieżą. Dodatkowo obejmuje wszystkie stacje robocze, drukarki oraz nośniki pamięci. Sekcja ″Planowanie ochrony fizycznej″ zawiera więcej informacji na temat planowania ochrony fizycznej, ryzyka oraz zaleceń firmy IBM.

Ochrona aplikacji
Ochrona aplikacji zajmuje się przechowywanymi w systemie aplikacjami oraz sposobem ich zabezpieczania przy równoczesnym udostępnianiu użytkownikom. Sekcja ″Planowanie ochrony aplikacji″ udostępnia szczegóły dotyczące opisywania aplikacji oraz ich konwencje nazewnictwa.

Ogólna strategia ochrony
Planowanie ogólnej ochrony obejmuje tworzenie planu ochrony, który dotyczy zarówno sytuacji obecnej, jak i przyszłych planów biznesowych. Sekcja ″Planowanie ogólnej strategii ochrony″ udostępnia więcej informacji przydatnych podczas określania strategii ochrony, jej poziomu, haseł oraz wartości systemowych.

Ochrona grupy użytkowników
Grupa użytkowników to grupa, która korzysta z tych samych aplikacji, w ten sam sposób. Planowanie ochrony grup użytkowników obejmuje określanie grup roboczych, które mają korzystać z systemu, oraz wymaganych przez nie aplikacji. Sekcja ″Planowanie grup użytkowników″ udostępnia szczegółowe informacje na temat identyfikowania grup użytkowników, planowania profili grupowych, wybierania wartości systemowych oraz określania środowiska użytkownika.

Ochrona pojedynczych użytkowników
Po określeniu potrzebnych grup użytkowników, można zaplanować pojedyncze profile użytkowników. Sekcja ″Planowanie pojedynczych profili użytkowników″ udostępnia więcej informacji na temat nazywania użytkowników w systemie, określania odpowiedzialności pojedynczych użytkowników oraz wybierania wartości systemowych.

W tematach dotyczących planowania można znaleźć odsyłacze do formularzy planowania, które można wykorzystać do zapisania swoich decyzji.

Planowanie ochrony fizycznej

Podczas przygotowywania się do zainstalowania systemu iSeries należy utworzyć plan ochrony fizycznej, udzielając odpowiedzi na następujące pytania:

- Gdzie zostanie umieszczona jednostka systemowa?
- Gdzie zostanie umieszczona każda stacja robocza?
- Gdzie zostaną umieszczone drukarki?
- Jaki sprzęt dodatkowy jest potrzebny (np. okablowanie, linie telefoniczne, meble lub obszary pamięci)?

- Jakie środki zostaną podjęte w celu zabezpieczenia systemu przed sytuacjami wyjątkowymi, takimi jak ogień lub przerwy w dostawie prądu?

Ochrona fizyczna powinna być częścią ogólnego planowania ochrony. W zależności od umiejscowienia systemu oraz jego urządzeń, mogą być potrzebne specjalne środki do ich zabezpieczenia.

W celu zapisania decyzji dotyczących ochrony fizycznej systemu można wykorzystać Formularz planowania ochrony fizycznej. Aby upewnić się, że ujęte zostały wszystkie aspekty ochrony fizycznej, należy zapoznać się z następującymi tematami:

- Ochrona fizyczna jednostki systemowej, który zawiera szczegóły dotyczące zabezpieczania samego systemu.
- Ochrona fizyczna dokumentacji systemowej oraz nośników pamięci, który zawiera informacje na temat zabezpieczania dokumentów systemowych oraz nośników pamięci.
- Ochrona fizyczna stacji roboczych, w którym omówiono sposoby zabezpieczania stacji roboczych.
- Ochrona fizyczna drukarek oraz zbiorów wydruków, który udostępnia szczegóły dotyczące fizycznego zabezpieczania drukarek oraz ich wydruków.
- Planowanie strategii ochrony, który wyjaśnia, jak przygotować wskazówki dla użytkowników oraz strategię ochrony.

Każda jednostka systemowa ma panel sterujący, służący do serwisowania komputera oraz przeprowadzania specjalnych operacji systemowych, takich jak włączanie i wyłączanie systemu. Aby zabezpieczyć się przed nieautoryzowanym dostępem do tych operacji systemowych, każda jednostka systemowa ma stacyjkę lub klucz elektroniczny. Zapewniają one pewną ochronę jednostki systemowej, ale nie zastąpią odpowiedniej ochrony fizycznej.

Ochrona fizyczna jednostki systemowej

Serwer iSeries nie wymaga oddzielnego pomieszczenia ze specjalną kontrolą środowiska. Jednostkę systemową często można spotkać na środku biura, gdzie dostęp do niej ma wiele osób. Klientom odpowiadają małe rozmiary oraz łatwość obsługi serwera iSeries; jednak cechy te mogą także wywołać ryzyko zagrożenia ochrony. Na przykład jedna osoba może ukraść jednostkę systemową lub usunąć z niej wartościowe komponenty.

Należy podjąć odpowiednie środki, aby upewnić się, że jednostka systemowa znajduje się w bezpiecznym miejscu. Najlepszą lokalizacją jest zamykane pomieszczenie, do którego ma dostęp niewielka grupa osób. A przynajmniej jednostka systemowa powinna znajdować się w miejscu, które może być zamknięte poza normalnymi godzinami pracy.

Niebezpieczeństwa związane z jednostką systemową

Oprócz ryzyka kradzieży jednostki systemowej lub jej komponentów, istnieje kilka innych niebezpieczeństw, które mogą powstać z powodu niewystarczającej ochrony fizycznej jednostki systemowej:

Niezamierzone przerwanie działania systemu
Wiele problemów związanych z ochroną ma związek z działaniem autoryzowanych użytkowników systemu. Przypuśćmy, że jedna ze stacji roboczych systemu zablokowała się. Operator systemu pojechał na spotkanie. Sfrustrowany użytkownik stacji roboczej idzie do jednostki systemowej myśląc, że ″Może jeśli nacisnę ten przycisk, to coś się naprawi.″ Ten przycisk może wyłączyć lub przeładować system w chwili, gdy uruchomionych będzie wiele zadań. Odtwarzanie częściowo zaktualizowanych plików może zająć kilka godzin. Aby zapobiec takiemu zdarzeniu, można wykorzystać stacyjkę jednostki systemowej.

Wykorzystanie dedykowanych narzędzi serwisowych (DST) do obejścia ochrony
Ochrona nie kontroluje funkcji serwisowych, które wykonuje system, ponieważ oprogramowanie systemu może nie działać poprawnie podczas wykonywania tych funkcji. Dobrze poinformowana osoba, która zna lub zgaduje identyfikator użytkownika oraz hasło do narzędzi serwisowych, może spowodować w systemie znaczne uszkodzenia. Aby dowiedzieć się więcej o narzędziach serwisowych, należy zapoznać się z tematem Narzędzia serwisowe w Centrum informacyjnym.

Zalecenia

- Jednostkę systemową najlepiej jest przechowywać w zamkniętym pokoju. Jeśli nie można tego zrobić, należy umieścić ją w miejscu, do którego nie mają dostępu osoby spoza przedsiębiorstwa. Dodatkowo należy wybrać takie

miejsce, gdzie odpowiedzialni pracownicy będą mogli ją monitorować. Przedstawione poniżej opcje ochrony fizycznej mogą pomóc zabezpieczyć jednostkę systemową przed przypadkowym lub zamierzonym manipulowaniem:

- Należy używać klucza elektronicznego lub blokady:
  - Jeśli system ma być uruchamiany bez klucza, tryb pracy ustaw na Normal (Normalny).
  - Jeśli do uruchamiania i zatrzymywania ma być wykorzystywana funkcja automatycznego włączania/wyłączania, tryb pracy ustaw na Auto (Automatyczny).
  - Wyjmij klucz i schowaj go w bezpiecznym miejscu.
- Natychmiast po zainstalowaniu systemu lub po użyciu przez personel serwisu, należy zmienić identyfikator użytkownika oraz hasło do narzędzi serwisowych (DST). Temat Narzędzia serwisowe w Centrum informacyjnym szczegółowo wyjaśnia, jak to zrobić.

Przed zaplanowaniem ochrony fizycznej dokumentacji systemowej oraz nośników pamięci można zapoznać się z przykładem planu ochrony jednostki systemowej przedsiębiorstwa JKL Toy.

Przykład: Formularz planowania ochrony fizycznej dla przedsiębiorstwa JKL Toy — część dotycząca jednostki systemowej: Poniżej przedstawiono przykład części dotyczącej jednostki systemowej z Formularza planowania ochrony fizycznej, który Sharon Jones wykorzystuje dla swojego systemu:

Tabela 3. Formularz planowania ochrony fizycznej dla przedsiębiorstwa JKL Toy: przykład jednostki systemowej

Formularz planowania ochrony fizycznej	
Przygotowany przez: Sharon Jones	Data: 9/2/99
Jednostka systemowa:	
Opis wytycznych ochrony w celu zabezpieczenia jednostki systemowej (takich jak zamknięty pokój):	Jednostka systemowa znajduje się w pomieszczeniu księgowych. W ciągu dnia księgowi zawsze są w tym pomieszczeniu i mogą kontrolować jednostkę systemową. Są także odpowiedzialni za drobną gotówkę i ważne zapisy. Po godzinach pracy pomieszczenie jest zamykane.
Jaka pozycja kluczyka jest zazwyczaj wykorzystywana?	Normalna
Gdzie jest przechowywany klucz?	Mały sejf w biurze Sharon.
Pozostałe komentarze dotyczące jednostki systemowej:	Jednostka systemowa będzie łatwo dostępna. Należy wspomnieć pracownikom w pomieszczeniu księgowych, aby nie majstrowali przy niej.

Po zaplanowaniu ochrony fizycznej jednostki systemowej można zaplanować ochronę fizyczną dokumentacji systemowej i nośników pamięci.

Ochrona fizyczna dokumentacji systemowej oraz nośników pamięci

Innym aspektem planu ochrony fizycznej jest przechowywanie ważnej dokumentacji systemowej oraz nośników pamięci. Dokumentacja systemowa obejmuje informacje, które firma IBM wysyła z systemem, informacje o haśle, formularze planowania oraz wszystkie raporty, które generuje system.

W zależności od systemu nośnikami pamięci mogą być taśmy, dyski CD dyskietki lub dyski DVD. Dokumentacja systemowa oraz nośniki pamięci powinny być przechowywane w siedzibie firmy oraz w innym miejscu, oddalonym od firmy. W razie katastrofy te informacje będą potrzebne do odtworzenia systemu. Poniższe informacje sugerują sposoby przechowywania dokumentacji systemowej oraz nośników pamięci. Po dokonaniu wyboru metody należy potrzebne informacje zapisać w sekcji Składowanie nośników oraz dokumentacji w Formularzu planowania ochrony fizycznej.

Bezpieczne przechowywanie dokumentacji systemu

Hasła narzędzi serwisowych oraz szefa ochrony są krytycznymi danymi dla działania systemu. Należy je zapisać i przechowywać w bezpiecznym i tajnym miejscu. Dodatkowo kopię tych haseł należy przechowywać w innym miejscu oddalonym od siedziby firmy, aby można było je wykorzystać podczas odtwarzania po katastrofie.

Aby ustrzec się przed skutkami katastrofy, należy rozważyć przechowywanie innej ważnej dokumentacji systemowej, takiej jak ustawienia konfiguracyjne lub biblioteki aplikacji, poza siedzibą firmy.

Bezpieczne przechowywanie nośników pamięci

Po zainstalowaniu systemu należy zaplanować regularne składowanie na taśmach lub innych nośnikach pamięci wszystkich informacji systemowych. W razie konieczności te kopie zapasowe umożliwią odzyskanie systemu. Kopie zapasowe także powinny być przechowywane poza siedzibą.

Niebezpieczeństwa

- Uszkodzenia nośników składowania: jeśli katastrofa lub wandale zniszczą systemowe nośniki składowania, poza wydrukowanymi raportami, nie będzie można odzyskać pozostałych informacji systemowych.
- Kradzież nośników składowania lub haseł: na nośnikach pamięci mogą być składowane poufne informacje biznesowe. Osoba posiadająca odpowiednią wiedzę może odtworzyć te informacje na innym komputerze oraz wydrukować je lub przetwarzać w inny sposób.

Zalecenia

- Wszystkie hasła oraz nośniki pamięci należy przechowywać w zamkniętej, ognioodpornej szafce.
- Kopie nośników pamięci przynajmniej raz na tydzień należy przenosić do innego, bezpiecznego budynku.

Przed zaplanowaniem fizycznej ochrony stacji roboczych można zapoznać się z przykładem planu ochrony dla składowania dokumentacji systemowej przedsiębiorstwa JKL Toy.

Przykład: Formularz planowania ochrony fizycznej dla przedsiębiorstwa JKL Toy — część dotycząca nośników składowania i dokumentacji: Sharon Jones z przedsiębiorstwa JKL Toy przygotowała sekcję dotyczącą nośników składowania i dokumentacji Formularza planowania ochrony fizycznej, tak jak przedstawiono to w poniższej tabeli:

Tabela 4. Formularz planowania ochrony fizycznej dla przedsiębiorstwa JKL Toy: przykład nośników składowania i dokumentacji

Formularz planowania ochrony fizycznej	
Przygotowany przez: Sharon Jones	Data: 9/2/99
Nośniki składowania i dokumentacja:	
Gdzie w siedzibie firmy przechowywane są taśmy kopii zapasowej?	W dużym, ognioodpornym sejfie.
Gdzie poza siedzibą firmy przechowywane są taśmy kopii zapasowej?	W ognioodpornym sejfie w biurze księgowym.
Gdzie przechowywane są hasła szefa ochrony, usług i narzędzi DST?	W biurze Johna Smitha w bezpiecznej kombinacji.
Gdzie jest przechowywana ważna dokumentacja systemowa, taka jak numer seryjny i konfiguracja?	W dużym sejfie poza siedzibą oraz w biurze księgowym.

Po zaplanowaniu ochrony pamięci i dokumentacji można zaplanować ochronę fizyczną stacji roboczych.

Planowanie ochrony fizycznej stacji roboczych

W większości przypadków wymaga się, aby wszyscy użytkownicy mogli wpisywać się z każdej dostępnej stacji roboczej oraz wykonywać wszystkie autoryzowane funkcje. Jednak jeśli niektóre stacje robocze są łatwo dostępne lub znajdują się na uboczu, w ustronnych miejscach, należy podjąć dodatkowe środki ostrożności. Na przykład stacje robocze, które mogą przechowywać naciśnięcia klawiszy oraz komputery osobiste wymagają szczególnej uwagi. Z poniższych informacji można skorzystać podczas wypełniania Części 2 (Ochrona fizyczna stacji roboczych i drukarek) Formularza planowania ochrony fizycznej.

Niebezpieczeństwa związane ze stacjami roboczymi

Używanie stacji roboczej w miejscu publicznym w celach nieautoryzowanych

Jeśli osoby spoza przedsiębiorstwa mogą łatwo uzyskać dostęp do określonych miejsc, potencjalnie mogą zobaczyć poufne informacje. Jeśli użytkownik systemu pozostawi stację roboczą bez wypisania się, ktoś spoza przedsiębiorstwa może wejść i uzyskać dostęp do poufnych informacji.

Używanie stacji roboczej w ustronnym miejscu w celach nieautoryzowanych

Stacja robocza znajdująca się w ustronnym miejscu daje intruzowi możliwość spędzenia wielu godzin na próbach obejścia ochrony bez ryzyka zauważenia.

Używanie funkcji odtwarzania lub programu z komputera PC do wpisywania się w stacji roboczej, w celu obejścia ochrony

Wiele stacji roboczych ma funkcję zapisywania i odtwarzania, która umożliwia użytkownikom zapisanie często używanych sekwencji klawiszy i powtarzanie ich przez naciśnięcie pojedynczego klawisza. Jeśli komputer osobisty jest wykorzystywany jako stacja robocza systemu iSeries można napisać program do zautomatyzowania procesu wpisywania się. Ponieważ użytkownicy często korzystają z procesu wpisywania się, mogą przechowywać swoje identyfikatory oraz hasła, zamiast wpisywać je podczas każdego logowania.

Zalecenia

Podczas konfigurowania ochrony fizycznej stacji roboczych, należy rozważyć następujące zalecenia:

- jeśli to możliwe, należy unikać umieszczania stacji roboczych w miejscach publicznych lub ustronnych,
- należy wyjaśnić użytkownikom systemu, jak ważne jest wypisywanie się przed pozostawieniem stacji roboczej; procedury wypisywania się powinny znaleźć się w strategii ochrony,
- należy wyjaśnić, że zapisywanie hasła w stacji roboczej lub programie komputera PC narusza ochronę systemu; informacje na temat zapisywania hasła powinny znaleźć się w strategii ochrony,
- należy podjąć środki, za pomocą wartości systemowych licznika czasu nieaktywności (QINACTITV i QINACTMSGQ), zapobiegające pozostawianiu stacji roboczych znajdujących się w miejscach publicznych przez użytkowników bez wypisywania się z systemu,
- należy ograniczyć funkcje, które użytkownicy mogą wykonywać na łatwo dostępnych stacjach roboczych, umożliwiając korzystanie z nich tylko użytkownikom z ograniczonymi uprawnieniami,
- za pomocą ochrony lub uprawnień serwisowych należy zapobiegać wpisywaniu się użytkowników na stacjach roboczych znajdujących się w ustronnych miejscach; za pomocą wartości systemowej QLMTSECOFR można sterować, gdzie użytkownik z określonymi uprawnieniami może wpisywać się do systemu,
- należy ograniczyć możliwość wpisywania się użytkowników na więcej niż jednej stacji roboczej w tym samym momencie; w tym celu można użyć wartości systemowej, która ogranicza liczbę sesji urządzeń (QLMTDEVSSN).

Aby zastosować te zalecenia, należy zapoznać się z tematem ″Wybieranie wartości systemowych, które wpływają na wpisywanie się″ oraz ″Planowanie ochrony zasobów stacji roboczych″.

W Formularzu planowania ochrony fizycznej należy podać, które stacje robocze, z powodu ich umiejscowienia, są narażone na największe ryzyko. Można zapoznać się z przykładem planowania ochrony fizycznej stacji roboczych przedsiębiorstwa JKL Toy przez Sharon Jones.

Po zaplanowaniu ochrony stacji roboczych, można zaplanować ochronę fizyczną drukarek oraz zbiorów wydruków.

Ochrona fizyczna drukarek oraz zbiorów wydruków

Po rozpoczęciu drukowania informacji ochrona systemu nie ma już wpływu na to, kto je zobaczy. Aby zminimalizować możliwość zobaczenia przez kogoś ważnych informacji biznesowych, należy zabezpieczyć drukarki oraz ich wydruki. Należy także utworzyć strategię, która będzie obejmowała drukowanie poufnych danych biznesowych.

Niebezpieczeństwa związane z drukarkami i zbiorami wydruków

Przedstawione poniżej niebezpieczeństwa mogą mieć zastosowanie do sytuacji biznesowej użytkownika. Są to najczęściej występujące niebezpieczeństwa związane z drukarkami i wydrukami. Jednak należy sprawdzić, czy w konkretnym przypadku nie istnieją inne niebezpieczeństwa.

- Drukarka znajdująca się w miejscu publicznym może umożliwić dostęp do poufnych informacji przez osoby nieautoryzowane.
- Wydruki pozostawione na biurku mogą ujawnić informacje.
- W systemie może być tylko jedna lub dwie drukarki. W takim przypadku podczas drukowania wartościowych lub poufnych informacji, na przykład list płac, mogą je zobaczyć pracownicy przedsiębiorstwa.

Zalecenia

Poniższe zalecenia mogą pomóc zmniejszyć ryzyko ochrony związane z drukarkami i wydrukami.

- należy wyjaśnić użytkownikom systemu, jak ważne jest zabezpieczanie poufnych wydruków; decyzje dotyczące ochrony fizycznej drukarek należy dołączyć do strategii ochrony,
- należy unikać umieszczania drukarek w miejscach publicznych,
- należy zaplanować drukowanie bardzo poufnych danych i podczas ich drukowania wysłać autoryzowaną osobę do pilnowania drukarki.

W sekcji ″Planowanie ochrony drukarek i zbiorów wydruków″ omówiono zalecenia dotyczące postępowania z wydrukami poufnymi.

Przed zaplanowaniem strategii ochrony można zapoznać się z przykładem planowania ochrony drukarek w przedsiębiorstwie JKL Toy.

Przykład: Formularz planowania ochrony fizycznej dla przedsiębiorstwa JKL Toy — część dotycząca stacji roboczych i drukarek: Poniżej przedstawiono przykład części 2 Planu ochrony fizycznej, którego Sharon Jones używa dla przedsiębiorstwa JKL Toy:

Tabela 5. Formularz planowania ochrony fizycznej dla przedsiębiorstwa JKL Toy: przykład stacji roboczej i drukarki

Formularz planowania ochrony fizycznej			Część 2 z 2
Ochrona fizyczna stacji roboczych i drukarek			
Nazwa stacji roboczej lub drukarki	Jej położenie lub opis	Ryzyko naruszenia ochrony	Podejmowane środki zabezpieczające
DSP06	Rampa załadowcza	Zbyt łatwo dostępna	Automatyczne wypisywanie się. Na stacji roboczej mogą być wykonywane ograniczone funkcje.
DSP09	Biuro obsługi klienta	Zbyt łatwo dostępna	Automatyczne wypisywanie się. Na stacji roboczej mogą być wykonywane ograniczone funkcje.
RMT12	Zdalne biuro sprzedaży	Zbyt słabo chroniona	Nie należy pozwalać szefowi ochrony wpisywać się na tej stacji.
PRT02	Księgowość, blisko jednostki systemowej	Często przetwarzane są informacje poufne, takie jak listy płac	Należy przydzielić kogoś do monitorowania wydruków

Po wypełnieniu Formularza planowania ochrony fizycznej, należy przejść do tematu ″Planowanie strategii ochrony″.

Planowanie strategii ochrony

Strategie ochrony dotyczące ochrony fizycznej oraz systemu powinny być znane wszystkim pracownikom, dlatego bardzo przydatne może być wysłanie wskazówek dotyczących ochrony do wszystkich pracowników. Te same wskazówki można przekazać nowym użytkownikom, którzy będą dodawani do systemu w późniejszym czasie.

W tych wskazówkach powinny być zawarte ogólne instrukcje dotyczące zabezpieczania systemu, takie jak wypisywanie się ze stacji roboczych oraz nieprzekazywanie haseł. Wskazówki powinny także zawierać informacje dotyczące określonych decyzji podjętych w celu ochrony.

Podczas czytania informacji dotyczących planowania należy notować, co powinny zawierać wskazówki dotyczące ochrony. Można także robić notatki dotyczące strategii ochrony.

Na przykład Sharon Jones z przedsiębiorstwa JKL Toy, podczas planowania ochrony fizycznej systemu, zrobiła następujące notatki do wskazówek dotyczących ochrony:

```
Upewnić się, żeby podkreślone zostało wypisywanie się ze stacji roboczych na rampie załadowczej,
biurze obsługi klienta oraz w zdalnych biurach sprzedaży. Księgowi będą pilnować jednostki systemowej.
```

Po wypełnieniu Formularza planowania ochrony fizycznej można przejść do planowania ochrony aplikacji.

Planowanie ochrony aplikacji

Aby zaplanować poprawną ochronę aplikacji, należy wiedzieć:

- Jakie informacje mają być przechowywane w systemie?
- Kto potrzebuje dostępu do tych informacji?
- Jakiego rodzaju dostępu potrzebują użytkownicy? Czy potrzebują oni zmieniać informacje, czy tylko je przeglądać?

Po zapoznaniu się z tymi tematami planowania aplikacji, znana będzie odpowiedź na pierwsze pytanie na temat tego, jakie informacje mają być przechowywane w systemie. W dalszych tematach należy określić osoby wymagające tych informacji oraz rodzaj dostępu do nich. Informacje planowania aplikacji nie są wprowadzane do systemu; jednak niektóre z nich będą potrzebne podczas konfigurowania ochrony użytkowników oraz zasobów.

Co to jest aplikacja?

W pierwszym kroku planowania ochrony aplikacji należy opisać aplikacje, które mają być uruchamiane w systemie. Aplikacja to grupa funkcji, które są połączone logicznie. Na przykład w przedsiębiorstwie JKL Toy wprowadzanie zamówień, dostarczanie zamówień oraz drukowanie faktur to część aplikacji nazwanej Przetwarzanie zamówień.

Zazwyczaj na serwerze iSeries mogą być uruchamiane dwa rodzaje aplikacji:

- **Aplikacje biznesowe**: aplikacje, które są kupowane lub tworzone w celu wykonywania określonych funkcji biznesowych, takich jak przetwarzanie zamówień lub zarządzanie zapasami.
- **Aplikacje specjalne**: aplikacje używane w przedsiębiorstwie do wykonywania różnych czynności, które nie są związane z prowadzeniem działalności.

Które formularze są potrzebne?

Wymienione poniżej formularze pomogą w zaplanowaniu ochrony aplikacji:

- Formularz opisywania aplikacji
- Formularz opisywania biblioteki
- Formularz konwencji nazewnictwa

Aby wydrukować te formularze, należy kliknąć odsyłacz, wybrać właściwą ramkę, a następnie kliknąć w przeglądarce ikonę **Drukuj**.

Poniższe tematy zawierają informacje pomocne przy wypełnianiu formularzy planowania.

- Opisywanie aplikacji
- Opisywanie konwencji nazewnictwa
- Opisywanie informacji dotyczących bibliotek
- Rysowanie diagramu aplikacji

Opisywanie aplikacji

Teraz należy zebrać kilka ogólnych informacji o każdej aplikacji biznesowej. Należy je wpisać w odpowiednie pola Formularza opisywania aplikacji, tak jak przedstawiono to poniżej. Te informacje będą przydatne w późniejszym czasie, podczas planowania ochrony grup użytkowników oraz aplikacji:

Nazwa i nazwa skrócona aplikacji
Należy podać krótką nazwę oraz nazwę skróconą, którą można wykorzystać jako skrót w formularzach oraz podczas nazywania obiektów wykorzystywanych przez aplikację.

Informacje opisowe
Należy krótko opisać, co robi ta aplikacja.

Menu podstawowe i biblioteka
Należy podać, które menu jest podstawowe przy dostępie do aplikacji. Należy wskazać bibliotekę, w której znajduje się to menu. Zazwyczaj menu podstawowe kieruje do innych menu, zawierających określone funkcje aplikacji. Użytkownicy lubią widzieć menu podstawowe swoich głównych aplikacji bezpośrednio po wpisaniu się do systemu.

Program początkowy i biblioteka
Czasami aplikacje uruchamiają program początkowy, który ustawia dla użytkownika informacje drugoplanowe lub sprawdza ochronę. Jeśli aplikacja ma program początkowy lub program konfiguracyjny, należy podać go w formularzu.

Biblioteki aplikacji
Każda aplikacja zazwyczaj ma główną bibliotekę dla swoich plików. Należy podać wszystkie biblioteki wykorzystywane przez aplikację, łącznie z bibliotekami programów oraz bibliotekami innych aplikacji. Na przykład aplikacja do obsługi zamówień klientów w przedsiębiorstwie JKL Toy korzysta z biblioteki zapasów, z której pobiera bilanse pozycji oraz opisy.

Powiązania między bibliotekami i aplikacjami można wykorzystać do określenia kto potrzebuje dostępu do danej biblioteki.

Znajdowanie informacji na temat aplikacji

Jeśli informacje na temat aplikacji nie są jeszcze znane, należy skontaktować się z programistą lub dostawcą aplikacji.

Poniżej przedstawiono metody samodzielnego zbierania informacji, w przypadku gdy nie ma dostępu do informacji na temat aplikacji, które działają w systemie.

- Użytkownicy aplikacji prawdopodobnie mogą podać nazwę menu podstawowego oraz biblioteki lub można obserwować ich wpisywanie do systemu.
- Jeśli program pojawia się natychmiast po wpisaniu się użytkownika do systemu, należy sprawdzić pole **Program początkowy** w profilu użytkownika. To pole zawiera program początkowy aplikacji. Aby przejrzeć program początkowy, można skorzystać z komendy DSPUSRPRF.
- Istnieje możliwość zapoznania się z listą nazw i opisów wszystkich bibliotek w systemie. W tym celu należy podać komendę DSPOBJD *ALL *LIB. Spowoduje to wyświetlenie wszystkich bibliotek w systemie.
- Podczas uruchamiania aplikacji przez użytkowników można obserwować aktywne zadania. Aby uzyskać szczegółowe informacje na temat zadań interaktywnych, należy skorzystać z komendy Praca z zadaniami aktywnymi (Work with Active Jobs - WRKACTJOB) z pośrednim poziomem asysty. Aby dowiedzieć się, które biblioteki są używane, należy wyświetlić zadania i sprawdzić listy bibliotek oraz ich blokady obiektów.
- Za pomocą komendy Praca z zadaniami użytkownika (Work with User Jobs - WRKUSRJOB) można wyświetlić zadania wsadowe aplikacji.

Aby upewnić się, że zostały zebrane wszystkie informacje potrzebne do zaplanowania ochrony aplikacji, przed kontynuowaniem należy wykonać następujące czynności:

- Wypełnij Formularz opisywania aplikacji dla każdej aplikacji biznesowej. Wypełnij cały formularz, z wyjątkiem sekcji wymagań ochrony. Ta sekcja zostanie użyta do zaplanowania ochrony zasobów dla aplikacji, tak jak opisano to w temacie ″Planowanie ochrony zasobów″.

- Przygotuj Formularz opisywania aplikacji dla każdej aplikacji specjalnej. Za pomocą formularza określ, w jaki sposób udostępnić aplikację.

Uwaga: Przygotowywanie Formularzy opisywania aplikacji dla aplikacji specjalnych z firmy IBM, takich jak program IBM Query for iSeries jest opcjonalne. Dostęp do bibliotek wykorzystywanych przez te aplikacje nie wymaga specjalnego planowania. Jednak zebranie informacji i przygotowanie formularzy może być przydatne.

Przed przejściem do opisywania konwencji nazewnictwa można zapoznać się z przykładem Formularza opisywania aplikacji przedsiębiorstwa JKL Toy.

Przykład: Formularz opisywania aplikacji dla przedsiębiorstwa JKL Toy: Sharon Jones na Formularzu opisywania aplikacji sporządziła listę wszystkich aplikacji w przedsiębiorstwie oraz ich nazwy skrócone. Opisała także krótko, jak z tymi aplikacjami pracują użytkownicy.

Zamówienia klientów (CO)
Wprowadzanie, śledzenie i dostarczanie zamówień. Drukowanie faktur.

Kontrola zapasów (IC)
Zarządzanie poziomem zapasów zarówno produktów finalnych jak i materiałów. Przetwarzanie wszystkich przesunięć między magazynami.

Kontrakty i wycena (CP)
Zarządzanie wyceną specjalną oraz kontraktami z klientami.

Należności (AC)
Śledzenie sald bieżących. Drukowanie zestawień miesięcznych.

Przedstawiona poniżej tabela zawiera opis aplikacji Zamówienia klientów, który został sporządzony przez Sharon Jones. Sharon przygotowywała swoje formularze systematycznie, opisując jedną aplikację, a potem następną.

Tabela 6. Formularz opisywania aplikacji dla przedsiębiorstwa JKL Toy: przykład

Formularz opisywania aplikacji	
Przygotowany przez: Sharon Jones	Data: 9/3/99
Nazwa aplikacji: Zamówienia klientów	Nazwa skrócona: CO
Krótki opis aplikacji:	Wprowadzanie zamówień klientów, śledzenie ich do czasu dostawy, dostarczanie zamówienia oraz drukowanie faktur i dokumentów dostawy.
Nazwa menu podstawowego: COMAIN	Biblioteka: COPGMLIB
Nazwa programu początkowego: NA	Biblioteka: NA
Lista bibliotek zbiorów, plików i programów używanych przez aplikację: • CUSTLIB • ITEMLIB • KONTRAKTY • COPGMLIB	
Zdefiniuj cele ochrony aplikacji, np. czy zawiera poufne informacje:	

Oprócz formularza dla aplikacji Zamówienia klientów, Sharon Jones przygotowała także Formularze opisywania aplikacji dla następujących aplikacji przedsiębiorstwa JKL Toy:

- Kontrola zasobów,
- Kontrakty i wycena,
- Należności.

Następnie można opisać konwencje nazewnictwa obiektów w systemie.

Opisywanie konwencji nazewnictwa

Kiedy już wiadomo, w jaki sposób system nadaje nazwy obiektom, można zaplanować i monitorować ochronę, rozwiązywać problemy oraz zaplanować tworzenie i odtwarzanie kopii zapasowych. Większość aplikacji ma zasady nadawania nazw obiektom, takim jak biblioteki, zbiory, pliki i programy. Jeśli aplikacje pochodzą z różnych źródeł, to prawdopodobnie mają własne unikalne systemy nazewnictwa.

Należy upewnić się, że w Formularzu konwencji nazewnictwa zapisane zostały wszystkie konwencje nazewnictwa aplikacji. W Formularzu konwencji nazewnictwa należy podać listę reguł wykorzystywanych przez aplikacje do nadawania nazw bibliotekom i plikom. Puste wiersze można wykorzystać do podania innych konwencji nazewnictwa, takich jak programy i menu. Jeśli aplikacje pochodzą z różnych źródeł, to prawdopodobnie mają unikalne systemy nazewnictwa. Należy opisać konwencje nazewnictwa każdej aplikacji. Może zaistnieć potrzeba przygotowania więcej niż jednego Formularza konwencji nazewnictwa.

Przed przejściem do opisywania informacji dotyczących bibliotek można zapoznać się z przykładem sposobu użycia przez Sharon konwencji nazewnictwa dla obiektów w systemie przedsiębiorstwa JKL Toy.

Przykład: Formularz konwencji nazewnictwa dla przedsiębiorstwa JKL Toy: Przedstawiona poniżej tabela prezentuje konwencje nazewnictwa tylko dla bibliotek, zbiorów i plików. Trzeba także opisać konwencje nazewnictwa dla innych rodzajów obiektów w systemie. Formularz konwencji nazewnictwa zawiera kilka wspólnych obiektów, jednakże w systemie użytkownika mogą być inne, dla których też trzeba przygotować formularz.

Tabela 7. Formularz konwencji nazewnictwa dla przedsiębiorstwa JKL Toy: przykład

Formularz konwencji nazewnictwa	
Przygotowany przez: Sharon Jones	Data: 9/3/99
Typ obiektu	**Konwencja nazewnictwa**
Biblioteki	Biblioteki zawierające pliki i zbiory mają jednoznaczne nazwy, takie jak KONTRAKTY lub ITEMLIB. Biblioteki programów korzystają z nazwy skróconej aplikacji z następującymi po niej znakami PGMLIB, na przykład ICPGMLIB.
Pliki	Główne zbiory mają jednoznaczne nazwy, na przykład CUSTMAST dla zbioru Customer Master (baza klientów) lub ITEMMAST dla pliku Item Master (baza produktów). Pozostałe pliki aplikacji (używane tylko w celach zrozumiałych dla programistów) mają nadawane nazwy w postaci nazwy skróconej aplikacji z następującym po niej napisem FILE i numerem, na przykład ICFILE14.

Po wypełnieniu Formularza konwencji nazewnictwa, można rozpocząć opisywanie informacji dotyczących bibliotek.

Opisywanie informacji dotyczących bibliotek

Po opisaniu konwencji nazewnictwa, należy opisać biblioteki w systemie. Biblioteki identyfikują oraz organizują obiekty w systemie. Umieszczenie podobnych plików w jednej bibliotece daje użytkownikom łatwy dostęp do krytycznych aplikacji oraz plików. Istnieje także możliwość dostosowania uprawnień użytkowników, tak aby mieli dostęp do pewnych bibliotek, ale nie mieli dostępu do innych. Należy opisać wszystkie biblioteki w systemie dla każdej aplikacji. Może zaistnieć potrzeba przygotowania więcej niż jednego Formularza opisywania biblioteki.

Uwaga: Należy podać tylko opisowe informacje dotyczące biblioteki. Jeśli planowana jest ochrona zasobów dla biblioteki, zostanie także wypełniona reszta Formularza opisywania biblioteki. Później trzeba będzie dodać informacje na temat uprawnień dla bibliotek. Szczegóły dotyczące wypełniania reszty Formularza opisywania biblioteki zawiera sekcja ″Planowanie ochrony bibliotek aplikacji″.

Przed kontynuowaniem należy upewnić się, że:

- w Formularzu konwencji nazewnictwa wypełnione zostały części dotyczące biblioteki i pliku,
- w Formularzu opisywania biblioteki dla każdej biblioteki aplikacji podane zostały informacje opisowe.

Przed narysowaniem diagramu aplikacji można zapoznać się z przykładem opisu bibliotek przedsiębiorstwa JKL Toy przez Sharon Jones.

Przykład: Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: Poniższe tabele pokazują dwie biblioteki, które wykorzystuje aplikacja Zamówienia klientów w przedsiębiorstwie JKL Toy. Pierwsza tabela prezentuje bibliotekę zawierającą zbiory, a druga bibliotekę zawierającą programy.

Tabela 8. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład biblioteki zawierającej zbiory

Formularz opisywania biblioteki	
Przygotowany przez: Sharon Jones	Data: 9/3/99
Nazwa biblioteki: CUSTLIB	Nazwa opisowa (tekst): Biblioteka klientów
Krótki opis funkcji tej biblioteki:	Przechowuje wszystkie zbiory klientów, w tym zamówienia i należności.

Tabela 9. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład biblioteki zawierającej programy

Formularz opisywania biblioteki	
Przygotowany przez: Sharon Jones	Data: 9/3/99
Nazwa biblioteki: COPGMLIB	Nazwa opisowa (tekst): Biblioteka programu Zamówienia klientów
Krótki opis funkcji tej biblioteki:	Przechowuje wszystkie programy dla aplikacji Zamówienia klientów.

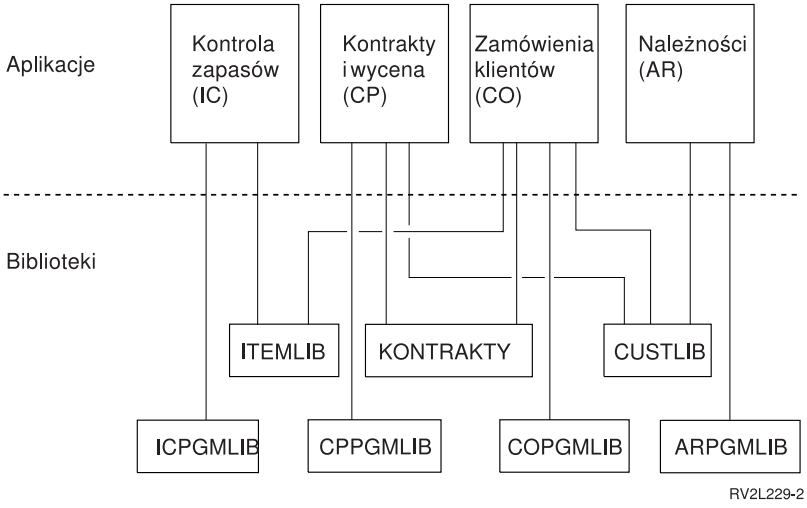
Po opisaniu bibliotek należy narysować diagram aplikacji dla systemu.

Rysowanie diagramu aplikacji

Po przygotowaniu Formularza opisywania aplikacji oraz Formularza opisywania biblioteki, przydatne może być narysowanie diagramu przedstawiającego powiązania między aplikacjami i bibliotekami. Diagram ułatwi zaplanowanie ochrony grup użytkowników oraz zasobów.

Przedstawiony poniżej rysunek prezentuje diagram narysowany przez Sharon Jones, który dotyczy aplikacji i bibliotek przedsiębiorstwa JKL Toy:

Diagram aplikacji i bibliotek przedsiębiorstwa JKL Toy



Zebranie niektórych informacji na temat aplikacji i bibliotek znacznie ułatwi podejmowanie wielu decyzji dotyczących ochrony. Możne to być szansa na powiększenie swojej wiedzy o systemie i aplikacjach.

Aby upewnić się, że zostały zebrane wymagane informacje o aplikacjach, należy:

- wypełnić Formularz opisywania aplikacji dla każdej aplikacji biznesowej w systemie,
- opcjonalnie wypełnić Formularz opisywania aplikacji dla każdej aplikacji specjalnej w systemie,
- w Formularzu konwencji nazewnictwa wypełnić sekcje dotyczące bibliotek i zbiorów,
- dla każdej biblioteki aplikacji przygotować Formularz opisywania biblioteki,
- narysować diagram powiązań między aplikacjami i bibliotekami.

Po wypełnieniu tych formularzy można zacząć planowanie ogólnej strategii ochrony.

Planowanie ogólnej strategii ochrony

Po zaplanowaniu ochrony aplikacji można rozpocząć planowanie ogólnej strategii ochrony. Najpierw należy podjąć decyzje odnośnie ogólnego podejścia do ochrony w systemie. Następnie należy porównać aktualne potrzeby przedsiębiorstwa oraz potrzeby, które pojawią się w przyszłości.

Te informacje będą pomocne podczas procesu planowania strategii ochrony i określania celów. Na podstawie tych informacji można także wybrać podstawowe wartości systemowe, które wpływają na wszystkich użytkowników w systemie.

Które formularze są potrzebne?

Aby zakończyć planowanie aplikacji, należy użyć Formularza wybierania wartości systemowych.

Aby dokonać wyboru wartości systemowych, podczas przeglądania poniższych tematów należy skorzystać z wypełnionego Formularza planowania ochrony fizycznej oraz Formularza opisywania aplikacji.

Aby zaplanować strategię ochrony, należy zapoznać się z następującymi tematami:

- Pisanie strategii ochrony
- Wybieranie poziomu ochrony
- Wybieranie wartości systemowych, które wpływają na wpisywanie się
- Wybieranie wartości systemowych, które wpływają na hasła
- Korzystanie z wartości systemowych podczas dostosowywania systemu

Pisanie strategii ochrony

Przed rozpoczęciem planowania należy przygotować instrukcję strategii dla przedsiębiorstwa dotyczącą ochrony systemu. Ta instrukcja to umowa między użytkownikiem a zarządem przedsiębiorstwa. Pomaga podejmować decyzje oraz określać, co jest ważne. Strategia ochrony powinna zawierać ogólne podejście oraz informacje o tym, które aktywa wymagają ochrony.

Każdy system powinien mieć ochronę. Do ochrony systemu można zastosować jedno z poniższych podejść:

- **Ścisłe**: niektórzy nazywają je schematem ochrony, który musi być znany. W środowisku ścisłej ochrony użytkownicy mają dostęp tylko do informacji i funkcji, które są im potrzebne. Pozostałe są wykluczane. Większość kontrolerów zaleca takie podejście.
- **Średnie**: średnie podejście do ochrony daje użytkownikom dostęp do obiektów w zależności od przypisanych im uprawnień.
- **Łagodne**: w łagodnym środowisku ochrony użytkownicy mają dostęp do większości obiektów w systemie. Dostęp jest ograniczany w przypadku określonych krytycznych lub poufnych zasobów. Pojedynczy dział lub małe przedsiębiorstwo zazwyczaj korzysta z łagodnego podejścia do swoich systemów.

Ogólne podejście pomaga w podejmowaniu decyzji dotyczących konkretnych potrzeb ochrony. Podejście do ochrony w systemie powinno być zgodne z filozofią dostępu do informacji w całym przedsiębiorstwie. Jeśli użytkownik nie jest pewien, jakiego podejścia powinien użyć, należy:

- skorzystać z Formularza opisywania aplikacji w celu określenia, kto powinien lub nie powinien mieć dostępu do tych aplikacji,

- sprawdzić technologie wykorzystywane w przedsiębiorstwie; na przykład, jeśli planuje się połączenie systemu z siecią Internet, należy skorzystać z bardziej zamkniętego środowiska ochrony, aby zabezpieczyć system przed użytkownikami z zewnątrz,
- porozmawiać z innymi pracownikami przedsiębiorstwa, takimi jak kontrolerzy ochrony, aby lepiej określić potrzeby ochrony.

Należy pamiętać, że strategię zawsze można zmienić. Większość przedsiębiorstw, w miarę rozrostu, potrzebuje bardziej ścisłej ochrony. Te informacje pomagają w skonfigurowaniu schematu ochrony, który umożliwia zwiększenie ochrony w przyszłości, bez konieczności wprowadzania dużych zmian lub ponownego testowania aplikacji.

Co należy chronić

Oprócz ustanowienia ogólnego podejścia do ochrony w danej strategii ochrony, należy także zidentyfikować krytyczne aktywa przedsiębiorstwa. System ochrony powinien zabezpieczać takie informacje. W celu określenia krytycznych aktywów, można skorzystać z kilku wymagań:

- **Poufność**: informacje, które nie są ogólnie dostępne dla osób w przedsiębiorstwie. Przykładem poufnych informacji jest lista płac.
- **Konkurencyjność**: informacje, które dają przewagę nad konkurencją, do których można zaliczyć specyfikacje oraz formuły.
- **Operacje**: informacje w komputerze, które są istotne dla codziennych operacji w firmie, takie jak zapisy dotyczące klientów oraz salda zapasów.

Sharon Jones, szef ochrony oraz John Smith, prezes przedsiębiorstwa, pracują razem nad instrukcją strategii ochrony. John Smith korzysta z tych notatek, aby nakreślić strategię ochrony dla przedsiębiorstwa JKL Toy. Można zapoznać się ze strategią ochrony, która zostanie wysłana do wszystkich pracowników przedsiębiorstwa JKL Toy po zakończeniu planowania i konfigurowania ochrony. Należy pamiętać, że podczas pracy z tematami planowania należy sporządzać notatki o tym, co powinno się znaleźć w strategii ochrony.

Tabela 10. Strategia ochrony dla przedsiębiorstwa JKL Toy: przykład

Podejście ogólne Łagodne: większość osób wymaga dostępu do większości informacji.
Informacje krytyczne • Kontrakty i ceny specjalne • Lista płac • Zapisy dotyczące klientów i zapasów są dostępne tylko dla pracowników przedsiębiorstwa.
Zasady ogólne • Każdy użytkownik systemu będzie miał profil użytkownika. Użytkownik nie może udostępniać profili ani haseł. • Użytkownik musi zmieniać swoje hasła co 60 dni.

Po zrobieniu notatek dotyczących strategii ochrony można wybrać poziom ochrony.

Wybieranie poziomu ochrony

Wartość systemowa QSECURITY umożliwia kontrolowanie wymagań dotyczących ochrony. Aby zrozumieć, jak działają poziomy ochrony, wyobraźmy sobie, że system tobudynek, do którego chcą wejść ludzie.

Poziom 20: zabezpieczenie hasłem

Poziom 20 oznacza pewną ochronę. Strażnik przy drzwiach budynku prosi o identyfikację oraz o podanie tajnego hasła. Tylko osoby podające oba parametry mogą wejść do budynku. Ale jeśli już dana osoba znajdzie się w budynku, może pójść gdziekolwiek i robić cokolwiek.

Jeśli ktoś podsłucha tajne hasło i użyje go, aby ominąć strażnika, nie będzie przed nim żadnej ochrony.

Poziom 30: hasło i ochrona zasobów

Poziom 30 daje to samo, co poziom 20 oraz pozwala kontrolować, kto może przejść do niektórych części budynku oraz co może tam zrobić. Niektóre części budynku mogą być publiczne, podczas gdy inne będą ograniczone przez strażników przy drzwiach.

Osobom z dostępem do zastrzeżonych sekcji można umożliwić wykonywanie dowolnych czynności lub wymagać od nich, aby żądały informacji od autoryzowanych urzędników (programów). Intruz, który dostanie się do środka za pomocą czyjegoś hasła, nadal może ominąć strażników wewnętrznych i uzyskać dostęp do zabezpieczonych sekcji.

Poziom 40: zabezpieczenie integralności

Na poziomie 40, dostępne są wszystkie zabezpieczenia z poziomu 30, ale system weryfikuje dostęp użytkownika. Strażnicy przy drzwiach wewnątrz budynku sprawdzają hasła i rejestrują wszystkich użytkowników wchodzących do pokoju.

Poziom 50: zaawansowane zabezpieczenie integralności

Na poziomie 50 strażnicy egzekwują bardziej wymagający zestaw reguł, aby zapobiec dostaniu się przez zastrzeżone drzwi osoby ze specjalną wiedzą, sprawdzając tożsamość każdego, kto się wpisuje.

Zalecenia

System iSeries dostarczany jest z ustawieniem poziomu ochrony 40. Poziom ochrony 40 jest najlepszym wyborem dla większości instalacji, bez względu na to, czy strategia ochrony jest ścisła, średnia, czy łagodna. Jeśli wybrano łagodne podejście, do większości zasobów w systemie można ustanowić dostęp publiczny. Korzystając od samego początku z poziomu 40, użytkownik ma większą elastyczność przy lepszym zabezpieczaniu systemu w przyszłości, bez konieczności wprowadzania jakichkolwiek zmian.

Jeśli aplikacje są kupowane, należy sprawdzić, czy dostawca aplikacji testował je dla poziomu 40. Niektóre aplikacje korzystają z operacji, które na poziomie 40 powodują błędy. Jeśli aplikacje nie zostały przetestowane na poziomie 40 lub 50, należy rozpocząć od poziomu 30. Aby sprawdzić, czy aplikacja protokołuje awarie uprawnień, należy skorzystać z funkcji kroniki kontroli. Jeśli nie, poziom można zmienić na 40 lub 50.

Poziom ochrony 50 chroni przed zdarzeniami, które normalnie nie występują w większości systemów. System podejmuje dodatkowe sprawdzanie zawsze podczas uruchamiania programów. Dodatkowe sprawdzanie może mieć negatywny wpływ na wydajność.

Po wpisaniu w Formularzu wybierania wartości systemowych wybranego poziomu ochrony można wybrać wartości systemowe, które wpływają na wpisywanie się.

Wybieranie wartości systemowych, które wpływają na wpisywanie się

Po wybraniu poziomu ochrony za pomocą wartości systemowych można zadecydować, co użytkownicy zobaczą na ekranach oraz jak będą współdziałać z systemem. W tym celu należy zaplanować te wartości systemowe oraz zapisać je w Formularzu wybierania wartości systemowych.

Przedstawiona poniżej tabela opisuje wartości systemowe wykorzystane w tym temacie.

Tabela 11. Wartości systemowe iSeries oraz ich opisy

Wartość systemowa	Opis
QMAXSIGN	Ogranicza liczbę kolejnych prób wpisywania się.
QMAXSGNACN	Określa czynność, jaką system podejmuje w przypadku osiągnięcia liczby kolejnych prób wpisywania się.
QLMTDEVSSN	Określa, czy użytkownik może wpisać się do więcej niż jednej stacji roboczej korzystając z tego samego profilu.
QINACTITV	Określa, kiedy system podejmuje działanie dla nieaktywnego zadania.

Tabela 11. Wartości systemowe iSeries oraz ich opisy (kontynuacja)

Wartość systemowa	Opis
QINACTMSGQ	Określa czynność podejmowaną przez system, kiedy interaktywne zadanie jest nieaktywne przez czas określony w wartości systemowej QINACTITV.
QDSCJOBITV	Steruje, czy i kiedy system kończy zadanie, które zostało tymczasowo odłączone.
QLMTSECOFR	Określa, że szef ochrony, który ma uprawnienia do wszystkich obiektów w systemie, może korzystać tylko z konkretnych urządzeń.

Ograniczanie liczby prób wpisywania się (QMAXSIGN i QMAXSGNACN): Liczbę prób wpisywania się do systemu oraz działania podejmowane przez system po osiągnięciu limitu prób wpisywania się, określają dwie wartości systemowe.

Wartość systemowa Maksymalna liczba prób wpisywania się (QMAXSIGN) ogranicza liczbę kolejnych niepoprawnych prób wpisania się, po której system podejmie odpowiednie działanie. Niepoprawna próba wpisania się oznacza, że ktoś próbuje użyć profilu użytkownika z niepoprawnym hasłem lub niewłaściwą autoryzacją dla stacji roboczej.

Wartość systemowa Działanie po maksymalnej liczbie prób wpisania się (QMAXSGNACN) określa, co system zrobi, gdy ktoś spróbuje wpisać się zbyt dużo razy z rzędu. Możliwe wartości to:

1 Zapobieganie kolejnej próbie wpisania się do urządzenia. Nazywane to jest blokowaniem urządzenia. Nikt nie będzie mógł wpisać się do tego urządzenia do czasu, aż autoryzowana osoba odblokuje je za pomocą komendy WRKCFGSTS. Ta opcja zazwyczaj nie jest wystarczającym zabezpieczeniem, szczególnie gdy próby wpisania się dokonywane są z komputera osobistego lub z systemu zdalnego.

Operator systemu lub ktokolwiek z uprawnieniem *USE może ponownie udostępnić urządzenie.

2 Zapobieganie przed kolejną próbą wpisania się przez profil użytkownika. Nazywane jest to blokowaniem profilu użytkownika. Nikt nie będzie mógł wpisać się za pomocą tego profilu do czasu włączenia go przez autoryzowaną osobę za pomocą komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF).

Aby włączyć profil użytkownika (zmienić status), użytkownik musi być administratorem ochrony z uprawnieniem do korzystania z profilu.

3 Wyłącza zarówno profil użytkownika, jak i urządzenie.

Niebezpieczeństwa i zalecenia

Niektórzy ″żartownisie″ traktują zgadywanie haseł i włamywanie do systemów jako rozrywkę. Ograniczając liczbę prób wpisywania się, można ograniczyć możliwość ich działania.

Wartość systemowa Maksymalna liczba prób wpisywania się (QMAXSIGN) określa liczbę dozwolonych prób. Należy ustawić wystarczająco wysoką wartość, aby uniknąć frustrowania użytkowników. Natomiast odpowiednio niska wartość powinna zniechęcić użytkowników przed niedbałym wpisywaniem i zabezpieczyć system przed potencjalnymi intruzami. Maksymalną liczbę prób wpisywania się należy ustawić między 3 a 5.

Zalecanym działaniem po maksymalnej liczbie prób wpisywania się (QMAXSGNACN) jest 3, chociaż wyłączenie urządzenia oraz profilu użytkownika może sprawić kłopot użytkownikom systemu. Stacja robocza znajdująca się w ustronnym miejscu może dać intruzowi możliwość spróbowania wielu różnych kombinacji profili użytkowników oraz haseł. Jeśli system nie ma stacji roboczych, których umiejscowienie wiązałoby się niebezpieczeństwem, wystarczającym zabezpieczeniem będzie wyłączenie profilu użytkownika.

Należy sprawdzić wypełniony Formularz ochrony fizycznej. Jeśli stacje robocze znajdują się w zdalnych miejscach lub istnieją zdalni użytkownicy (którzy mają dostęp do systemu przez linie telefoniczne lub połączenia VPN), wtedy należy

ograniczyć limit prób wpisywania się. Należy upewnić się, że wybrane ustawienia wartości systemowych QMAXSIGN i QMAXSGNACN zostały dodane do części 2 Formularza wybierania wartości systemowych.

Przed wybraniem wartości systemowych, które w danym momencie ograniczają użytkownikom dostęp tylko do jednej stacji roboczej, przydatne może być zapoznanie się z przykładem, który ilustruje, jak te wartości systemowe współdziałają w celu ograniczenia prób wpisywania się.

Przykład: ograniczanie prób wpisywania się: Sharon Jones ograniczyła liczbę prób wpisywania się do 3 (QMAXSIGN ma wartość 3) i ustawiła wyłączanie zarówno profilu jak i urządzenia, jeśli limit zostanie przekroczony (QMAXSGNACN ma wartość 3). Poniżej przedstawiono co może się stać, gdy te wartości zostaną osiągnięte:
1. Roger dwa razy niepoprawnie wpisuje swoje hasło.
2. Po drugiej próbie otrzymuje komunikat ostrzegający, że kolejne niepoprawne wpisanie spowoduje wyłączenie profilu użytkownika.
3. Robi kolejną pomyłkę.
4. System wyłącza jego profil, a stacja robocza nie wyświetla już ekranu wpisywania się. Roger próbuje wpisać się do innej stacji roboczej, ale otrzymuje komunikat o błędzie.
5. Teraz musi poprosić Sharon o włączenie jego profilu. Sharon lub operator systemu musi także udostępnić stację roboczą Rogera. Jeśli Roger nie pamięta swojego hasła, Sharon nadaje mu hasło tymczasowe, które musi być zmienione po wpisaniu się.

Teraz można zapoznać się z wartością systemową, która ogranicza możliwość wpisywania się użytkowników do jednej stacji roboczej w tym samym czasie.

Ograniczanie użytkowników do jednej stacji roboczej w tym samym czasie: Wartość systemowa ograniczania sesji urządzeń (QLMTDEVSSN) określa, czy ten sam użytkownik może być wpisany do więcej niż jednej stacji roboczej w tym samym czasie. Możliwe wartości to:

0 System umożliwia wpisywanie nieograniczonej liczby użytkowników za pomocą tego samego profilu.

1 Profil użytkownika może być używany tylko na jednym urządzeniu jednocześnie. Użytkownik może mieć więcej niż jedną sesję na tym samym urządzeniu.

Niebezpieczeństwa i zalecenia

Umożliwienie wpisywania się tylko do jednej stacji roboczej lansuje dobre zwyczaje dotyczące ochrony. Leniwe zwyczaje powodują ryzyko związane z ochroną:
- ograniczenie użytkowników do jednego urządzenia zniechęca do współużytkowania identyfikatorów użytkowników i haseł; jeśli pracownicy współużytkują identyfikatory, następuje utrata kontroli i odpowiedzialności; nie będzie można sprawdzić, kto naprawdę uruchamiał daną funkcję w systemie,
- użytkownicy muszą pamiętać o wypisaniu się z jednej stacji roboczej, przed przejściem do innej; stacje robocze z podanymi informacjami logowania, ale nieużywane, stanowią zagrożenie ochrony.

Zalecanym ustawieniem wartości systemowej QLMTDEVSSN jest ustawienie 1, które ogranicza użytkowników do pojedynczego urządzenia. Użytkownikom systemu należy nadać unikalne identyfikatory użytkownika, hasła oraz uprawnienia, a następnie ograniczyć im możliwość korzystania z więcej niż jednej stacji roboczej w tym samym czasie. Należy upewnić się, że wybrane ustawienie wartości systemowej QLMTDEVSSN zostało dodane do części 2 Formularza wybierania wartości systemowych.

Teraz można rozpocząć planowanie wartości systemowych dla nieaktywnych zadań.

Planowanie wartości systemowych dla nieaktywnych zadań: Wartości systemowe współdziałają ze sobą, w celu określenia, jakie działanie musi podjąć system w przypadku, gdy użytkownik zapomni wypisać się ze stacji roboczej.

Interwał czasowy nieaktywności zadania (QINACTITV)
Wartość systemowa QINACTITV określa, czy system podejmie działanie, jeśli wpisano się do stacji roboczej, ale była ona nieaktywna przez określony czas.

Uwaga: **Nieaktywna** oznacza, że użytkownik przez określony czas nie nacisnął klawisza Enter lub klawisza funkcyjnego.

Kolejka komunikatów nieaktywnego zadania (QINACTMSGQ)
Ustawienie wartości systemowej QINACTMSGQ określa co system zrobi, gdy upłynie czas określony w wartości systemowej QINACTITV. W przypadku wybrania wartości ENDJOB, system zakończy wszystkie zadania, które były nieaktywne dłużej niż limit czasu podany w wartości systemowej QINACTITV. W przypadku DSCJOB, system odłączy nieaktywne zadanie. Jeśli podana zostanie nazwa kolejki komunikatów, a zadanie będzie nieaktywne przez dłuższy czas, system wyśle do niej komunikat ostrzegawczy.

Kiedy system **odłącza** zadanie w stacji roboczej, oznacza to, że tymczasowo je zawiesza. Na stacji roboczej pojawia się ekran wpisywania. Odłączone zadanie jest wznawiane, gdy ten sam użytkownik wpisuje się ponownie do tej samej stacji roboczej.

Interwał czasowy przed przerwaniem odłączonych zadań (QDSCJOBITV)
Wartość systemowa QDSCJOBITV steruje, czy i kiedy system kończy zadanie, które zostało tymczasowo odłączone. Zadania mogą być odłączane automatycznie, jako wynik działania wartości systemowych QINACTITV i QINACTMSGQ. Za pomocą opcji w menu Asysta Operacyjna lub komendy Odłączenie zadania (Disconnect Job - DSCJOB) użytkownicy mogą żądać, aby och zadania były tymczasowo wypisywane (odłączane).

Niebezpieczeństwa i zalecenia

Jeśli Sharon zapomni wypisać się ze stacji roboczej, John może do niej podejść i wykonać dowolne funkcje, do których jest uprawniona Sharon.

Nieaktywnymi stacjami roboczymi należy sterować bardzo uważnie z dwóch powodów:

- zastosowano ścisłe środowisko ochrony, a w systemie przechowywane są poufne informacje,
- stacje robocze znajdują się w miejscach, do których mają dostęp osoby spoza przedsiębiorstwa.

Pracę użytkowników przy stacjach roboczych często przerywają zwykłe obowiązki. Skorzystanie ze współdziałania wymienionych powyżej wartości systemowych umożliwi użytkownikom przerywanie pracy oraz zapewni ochronę systemu.

Aby wyeliminować te niebezpieczeństwa, firma IBM zaleca jednoczesne korzystanie z wartości systemowych QINACTITV, QINACTMSGQ, i QDSCJOBITV, co umożliwi użytkownikom przerywanie pracy oraz zapewni ochronę systemu.

Interwał czasowy nieaktywności zadania (QINACTITV): musi być wystarczająco krótki, aby zniechęcać przed pozostawianiem stacji roboczej bez nadzoru, ale nie za krótki, aby nie sprawiać kłopotu użytkownikom. Zalecane ustawienie to 30 minut. Gdy zadanie będzie nieaktywne przez 30 minut, system podejmie działanie określone w kolejce komunikatów nieaktywnego zadania.

Kolejka komunikatów nieaktywnego zadania (QINACTMSGQ): należy wybrać odłączanie zadania. System odłącza wszystkie zadania, które były nieaktywne przez okres podany w wartości systemowej interwał czasowy nieaktywności zadania. System zawiesza zadanie i wypisuje stację roboczą. Gdy ten sam użytkownik wpisze się ponownie, zadanie będzie kontynuowane tam gdzie zostało pozostawione.

Jest to najwygodniejsze rozwiązanie dla użytkowników, ponieważ system zawiesza zadanie, a nie kończy je. Odłączanie nieaktywnego zadania zapewnia taką samą ochronę systemu, jak kończenie zadania.

Uwaga: System nie może odłączać niektórych zadań. Jeśli system nie może odłączyć nieaktywnego zadania, jest ono kończone. Może to powodować utratę danych. Należy rozważyć ustawienie wartości systemowej QINACTMSGQ tak, aby wysyłała komunikaty do kolejki komunikatów operatora systemu.

Interwał czasowy przed przerwaniem odłączonego zadania (QDSCJOBITV): należy zachęcać użytkowników do tymczasowego wypisywania się z systemu, w momencie gdy muszą odejść od stacji roboczych na krótki czas oraz do kończenia zadania i wypisywania się, gdy muszą odejść na dłuższy czas.

Wartości systemowej QDSCJOBITV należy używać do odłączania zadań zanim system rozpocznie nocne przetwarzanie, takie jak automatyczne czyszczenie. Musi być wystarczająco długa, aby użytkownik mógł powrócić w ciągu dnia roboczego, ale odpowiednio krótka, aby zadania zostały zakończone przed rozpoczęcie przetwarzania nocnego. 300 minut (pięć godzin) jest odpowiednią wartością, pozwalającą na zakończenie przetwarzania nocnego bez wpływania na zadanie użytkownika.

Uwaga: Aby zapobiec próbom zmiany tych samych informacji przez dwóch użytkowników, system **blokuje** rekord przed jego aktualizacją. Gdy system odłącza zadanie użytkownika, wszystkie blokady zasobów pozostają. W zależności od projektu aplikacji oraz liczby użytkowników w systemie, blokady mogą powodować problemy związane z wydajnością systemu. Należy ustalić z programistą lub dostawcą aplikacji, czy blokowanie może mieć wpływ na wydajność.

Można zapoznać się z przykładem współdziałania wartości systemowych opisanych w tym temacie, aby sprawdzić, jak obsługują nieaktywne zadania.

Po zapisaniu w Formularzu wybierania wartości systemowych decyzji dotyczących nieaktywnych zadań, można zadecydować, jak ograniczyć możliwość wpisywania się przez szefa ochrony.

Przykład: obsługa zadań nieaktywnych za pomocą wartości systemowych QINACTITV, QINACTMSGQ i QDSCJOBITV: Przyjmijmy, że interwał czasowy nieaktywności zadania (QINACTITV) ustawiono na 30 minut. Po czasie system odłącza zadania nieaktywne (QINACTMSGQ ma wartość DSCJOB). Interwał czasowy przed przerwaniem odłączonych zadań (QDSCJOBITV) wynosi 300 minut (5 godzin). Na przykład, jeśli Sharon zapomni wypisać się o 9:30 rano, system odłączy jej zadanie o 10:00 rano i przerwie je o 3:00 po południu.

Dla wartości systemowych QINACTITV, QINACTMSGQ i QDSCJOBITV należy podać wartości ustalone podczas wypełniania części 2 Formularza wybierania wartości systemowych.

Po zapisaniu w Formularzu wybierania wartości systemowych decyzji dotyczących nieaktywnych zadań, można zadecydować, w jaki sposób ograniczyć możliwość wpisywania się przez szefa ochrony.

Ograniczanie miejsc, w których szef ochrony może się wpisać: Może zaistnieć potrzeba ograniczenia dostępu do pewnych stacji roboczych użytkownikom mającym uprawnienia do zmiany ochrony oraz sterowania obiektami. Zapobiega to wpisywaniu się tych użytkowników do stacji roboczych w zdalnych miejscach bez wiedzy szefa ochrony. Umożliwia to wartość systemowa QLMTSECOFR (ograniczenie dostępu dla szefa ochrony). Po ustawieniu wartości QLMTSECOFR na 1, użytkownicy z uprawnieniami specjalnymi do wszystkich obiektów (*ALLOBJ) lub serwisowymi (*SERVICE) mogą wpisać się tylko na konsoli lub innej wyznaczonej stacji roboczej.

Wartość systemowa QLMTSECOFR ogranicza możliwość wpisywania się szefa ochrony, użytkowników z uprawnieniami do wszystkich obiektów w systemie oraz personel serwisowy tylko do konsoli. Aby umożliwić tym użytkownikom dostęp do innych urządzeń, można skorzystać z komendy Nadanie uprawnień dla obiektu (Grant Object Authority - GRTOBJAUT).

Uwaga: Aby wartość systemowa QLMTSECOFR była aktywna, poziom ochrony systemu musi być równy 30 lub wyższy.

Niebezpieczeństwa i zalecenia

Wartość systemową QLMTSECOFR należy ustawić na 1. Jeśli ktoś podsłucha lub zgadnie hasło użytkownika z profilem szefa ochrony, będzie musiał mieć dostęp do urządzenia, które pozwoli mu wpisać się.

Po wpisaniu w części 2 Formularza wybierania wartości systemowych wyboru dotyczącego wartości systemowej QLMTSECOFR, można wybrać wartości systemowe wpływające na hasła.

Wybieranie wartości systemowych, które wpływają na hasła

Przypisywanie haseł należy umożliwić użytkownikom, a nie szefowi ochrony. Kiedy użytkownicy tworzą własne hasła, zazwyczaj nie muszą ich zapisywać. Hasła zapisane na kartce często są przechowywane w widocznych miejscach, co stanowi niebezpieczeństwo dla ochrony.

Wskazówka dotycząca tworzenia haseł

Użytkownicy mogą mieć problem z wymyślaniem dobrych haseł. Należy zasugerować następującą technikę: należy używać zdania, które łatwo zapamiętać i które pomaga utworzyć hasło trudne do odgadnięcia. Na przykład po urlopie można użyć zdania ″W Lubiatowie 4-tego lipca było kiepska pogoda″, co utworzy hasło WL4LBKP.

Na hasła wpływa kilka wartości systemowych. Można ustalić, jak często użytkownicy mają zmieniać hasła. Można także ustanowić wiele reguł zapobiegających używaniu haseł, które łatwo można zgadnąć. Wiele z tych wartości systemowych jest istotnych dla dużych organizacji. Kilka jest ważnych dla wszystkich.

Użycie opcji w menu ASSIST lub komendy Zmiana hasła (Change Password - CHGPWD), umożliwia użytkownikom przypisywanie sobie haseł. Kiedy użytkownicy zmieniają swoje hasła, system sprawdza nowe hasło używając wartości systemowych. Jeśli użytkownik zmienia hasło za pomocą komendy CHGUSRPRF, system nie sprawdza nowego hasła pod kątem wartości systemowych.

Uwaga: Jeśli ustawiona została jakakolwiek wartość systemowa dotycząca hasła, system nie umożliwi podania hasła, które będzie takie samo, jak nazwa profilu użytkownika, chyba że do ustawienia hasła użyta zostanie komenda CHGUSRPRF.

Przedstawiona poniżej tabela zawiera wartości systemowe, które wpływają na hasło oraz ich definicje:

Tabela 12. Wartości systemowe iSeries związane z hasłami

Wartość systemowa	Opis
QPWDEXPITV	Wymaga od użytkowników zmiany ich haseł po określonym czasie.
QPWDMAXLEN	Umożliwia określenie maksymalnej długości haseł.
QPWDMINLEN	Umożliwia określenie minimalnej długości haseł.
QPWDRQDDIF	Zapobiega używaniu dwóch haseł na zmianę.

Przedstawione poniżej tematy zawierają bardziej szczegółowe informacje na temat powyższych wartości systemowych:

- Określanie czasu ważności hasła
- Określanie długości hasła
- Ograniczanie powtórzeń haseł

Aby zapoznać się z dokumentacją w postaci elektronicznej dotyczącą wartości systemowych zaczynających się od znaków QPWD, w wierszu komend CL należy wpisać WRKSYSVAL *SEC.

Określanie czasu ważności hasła: Wartość systemowa QPWDEXPITV określa, jak często użytkownicy muszą zmieniać swoje hasła.

System ostrzega, kiedy hasło zbliża się do daty wygaśnięcia. Jeśli hasło utraci ważność, system poprosi użytkownika o zmianę hasła podczas następnego wpisywania się.

Zalecenia

Użytkownik powinien okresowo zmieniać swoje hasła. Zniechęci to do współużytkowania haseł z innymi użytkownikami systemu. Również gdy niepowołany użytkownik nauczy się czyjegoś hasła, to hasło będzie działało

tylko przez krótki okres czasu. Czas ważności hasła musi być wystarczająco długi, aby nie powodować irytacji użytkowników, ale wystarczająco krótki, aby zapewnić dobrą ochronę. Aby uniknąć tych problemów, powinien wynosić od 45 do 60 dni.

Po wpisaniu w części 2 Formularza wybierania wartości systemowych wyboru dokonanego dla wartości systemowej QPWDEXPITV można określić długość hasła.

Określanie długości hasła: Niektórzy użytkownicy nie lubią pisać. Jeśli się im pozwoli, to wybiorą jednoliterowe hasło lub swoje inicjały. Niestety krótkie hasła są łatwiejsze do odgadnięcia przez intruzów. Wartość systemowa QPWDMINLEN umożliwia ustawienie minimalnej długości dla wszystkich haseł w systemie.

Jeśli dany system komunikuje się z innymi systemami, użytkownicy mogą wymieniać hasła między dwoma komputerami. Niektóre metody komunikacji ograniczają hasło do maksymalnie 8 znaków. Wartość systemowa QPWDMAXLEN umożliwia określenie maksymalnej długości hasła.

Zalecenia

Minimalną długość hasła należy ustawić na 6. Spowoduje to wyeliminowanie możliwości stosowania inicjałów i zachęci użytkowników do większej kreatywności przy wyborze hasła. Jeśli system komunikuje się z innymi systemami, maksymalną długość hasła należy ustawić na 8.

Po wpisaniu w części 2 Formularza wybierania wartości systemowych wyborów dotyczących wartości systemowych QPWDMINLEN i QPWDMAXLEN, można zdecydować, jak ograniczyć powtarzanie haseł.

Ograniczanie powtórzeń haseł: Komenda Zmiana hasła (Change Password - CHGPWD) wymaga, żeby nowe hasło było inne niż poprzednie. Jednak dopóki nie zostanie użyta wartość systemowa QPWDRQDDIF, można ciągle korzystać z wymiany tylko dwóch haseł. Przedstawiona poniżej tabela przedstawia wybory dotyczące wartości systemowej QPWDRQDDIF:

Tabela 13. Ustawienia wartości systemowej QPDRQDDIF

Wartość	Liczba haseł sprawdzanych, czy się nie powtarzają
0	Dozwolonych jest 0 powtarzających się haseł.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Zalecenia

Aby zapewnić, że hasła będą unikalne przez rok, należy korzystać z wartości systemowych okresu ważności hasła oraz powtarzania hasła. Na przykład jeśli hasło wygasa po 60 dniach, dla wartości systemowej QPWDRQDDIF należy wybrać 7.

Po wpisaniu w części 2 Formularza wybierania wartości systemowych wyboru dotyczącego wartości systemowej QPWDRQDDIF, można zadecydować, jak korzystać z wartości systemowych do dostosowywania systemu.

Korzystanie z wartości systemowych w celu dostosowania systemu

System iSeries korzysta z wartości systemowych oraz atrybutów sieciowych do sterowania parametrami, również nie związanymi z ochroną. Programiści systemu oraz aplikacji korzystają z większości z tych wartości systemowych oraz atrybutów. Szef ochrony powinien w celu dostosowania systemu ustawić kilka wartości systemowych oraz atrybutów sieciowych.

Nadawanie nazwy systemowi

Do przypisania nazwy systemowi używany jest atrybut sieciowy SYSNAME. Nazwa systemu pojawia się w prawym górnym rogu ekranu wpisywania się oraz w raportach systemowych. Używana jest także podczas komunikacji z innym systemem lub komputerem osobistym za pomocą programu iSeries Access for Windows.

Kiedy system komunikuje się z innymi systemami lub komputerami osobistymi, nazwa systemu identyfikuje i odróżnia dany system od innych znajdujących się w sieci. Komputery wymieniają nazwy systemów za każdym razem, gdy komunikują się. Po przypisaniu nazwy systemowi nie należy jej zmieniać, gdyż zmiana wpływa na inne systemy w sieci.

Zalecenia

Dla systemu należy wybrać sensowną i unikalną nazwę. Nawet jeśli dzisiaj system nie komunikuje się z innymi komputerami, może to robić w przyszłości. Jeśli system jest częścią sieci, administrator tej sieci prawdopodobnie powie, jakiej nazwy należy użyć.

Na przykład Sharon Jones z przedsiębiorstwa JKL Toy zadecydowała, że system będzie miał nazwę JKLTOY.

Wyświetlanie godziny i daty w systemie

Istnieje możliwość podania, w jakiej kolejności będzie wyświetlany rok, miesiąc i dzień, gdy system będzie drukował lub wyświetlał datę. Można także określić, jaki znak będzie wstawiany między rokiem (Y), miesiącem (M) i dniem (D).

Wartość systemowa QDATFMT określa format daty. Poniższa tabela pokazuje wszystkie możliwe sposoby wydrukowania przez system daty, 16. lipca 2000:

Tabela 14. QDATFMT (formaty daty systemowej)

Wybór użytkownika	Opis	Rezultat
YMD	Rok, miesiąc, dzień	00/06/16
MDY	Miesiąc, dzień, rok	06/16/00
DMY	Dzień, miesiąc, rok	16/06/00
JUL	Data juliańska	00/168

Uwaga: Powyższe przykłady jako separator daty wykorzystują ukośnik (/).

Wartość systemowa QDATSEP określa, jaki znak jest używany do oddzielenia roku, miesiąca i dnia. Poniższa tabela pokazuje dostępne możliwości. Do określenia wyboru wykorzystywana jest liczba:

Tabela 15. QDATSEP (separator daty systemowej)

Znak separatora	Wartość QDATSEP	Rezultat
/ (ukośnik)	1	16/06/00
- (myślnik)	2	16-06-00
. (kropka)	3	16.06.00
, (przecinek)	4	16,06,00
(odstęp)	5	16 06 00

Uwaga: W powyższych przykładach wykorzystany został format DMR.

Wartość systemowa QTIMSEP określa, jaki znak wykorzystywany jest do oddzielenia godzin, minut i sekund podczas wyświetlania godziny. Do określenia wyboru wykorzystywana jest liczba. W poniższej tabeli pokazano, w jaki sposób, za pomocą każdej wartości, zostanie sformatowana godzina 10:30 rano:

Tabela 16. QTIMSEP (separator godziny systemowej)

Znak separatora	QTIMSEP	Rezultat
: (dwukropek)	1	10:30:00
. (kropka)	2	10.30.00
, (przecinek)	3	10,30,00
(odstęp)	4	10 30 00

Decydowanie, w jaki sposób nazwać urządzenia systemowe

System automatycznie konfiguruje wszystkie nowe stacje robocze oraz podłączone do nich drukarki. Nadaje on nazwę każdemu nowemu urządzeniu. Wartość systemowa QDEVNAMING określa, w jaki sposób przypisywane są nazwy. Poniższa tabela pokazuje sposób nadawania nazw przez system trzeciej stacji roboczej oraz drugiej drukarce podłączanym do systemu:

Tabela 17. Nazywanie urządzeń systemowych

Wybór użytkownika	Format nazwy	Nazwa stacji roboczej	Nazwa drukarki
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	Adres urządzenia	DSP010003	PRT010002

Uwaga: W powyższym przykładzie stacja robocza i drukarka podłączone są do pierwszego kabla.

Zalecenia

Należy korzystać z konwencji nazewnictwa systemu iSeries, chyba że uruchamiane jest oprogramowanie wymagające nazewnictwa systemu S/36. Nazwy systemu iSeries dla terminali i drukarek są znacznie wygodniejsze niż nazwy korzystające z adresu urządzenia. Nazwy stacji roboczej i drukarki pojawiają się na kilku ekranach Asysty Operacyjnej. Nazwy drukarek używane są także do zarządzania wydrukami.

Po skonfigurowaniu przez system nowego urządzenia należy użyć komendy Zmiana terminalu (Change Display Device - CHGDEVDSP) lub Zmiana drukarki (Change Printer Device - CHGDEVPRT), aby podać sensowny opis urządzenia. W opisie należy podać adres fizyczny urządzenia oraz jego położenie, na przykład *biuro Johna Smitha, linia 1 adres 6*.

Wybieranie drukarki systemowej

Aby przypisać drukarkę systemową, należy skorzystać z wartości systemowej QPRTDEV. Ta wartość, profil użytkownika oraz opis zadania określają, z której drukarki korzysta zadanie. Zadanie korzysta z drukarki systemowej, chyba że w profilu użytkownika lub opisie zadania zostanie podana inna drukarka.

Zalecenia

Normalnie drukarką systemową powinna być najszybsza drukarka w danym systemie. Drukarki systemowej należy używać do tworzenia długich raportów lub wydruków systemowych.

Uwaga: Nazwy drukarek nie będą znane do czasu zainstalowania i skonfigurowania systemu. Teraz należy zanotować położenie drukarki. Nazwę będzie można uzupełnić w późniejszym czasie.

Umożliwianie wyświetlania zakończonego wydruku

System umożliwia użytkownikom odszukanie swoich wydruków. Ekran Praca z wydrukami (Work with Printer Output) pokazuje wszystkie wydruki, które są aktualnie drukowane lub czekają na drukowanie. Można także umożliwić użytkownikowi przeglądanie listy zakończonych wydruków. Ten ekran prezentuje informacje, kiedy wydruk miał miejsce oraz na której drukarce. Ta funkcja może być przydatna podczas szukania zaginionych raportów.

Funkcja rozliczania zadania oraz wartość systemowa QACGLVL umożliwiają wyświetlanie zakończonych wydruków. Opcja *PRINT wartości systemowej QACGLVL umożliwia zapisanie informacji na temat zakończonych wydruków.

Zalecenia

Składowanie informacji na temat zakończonych wydruków zajmuje przestrzeń w systemie. O ile użytkownicy nie będą drukowali wielu raportów, prawdopodobnie ta funkcja nie będzie musiała być udostępniana. W Formularzu wybierania wartości systemowych należy wpisać NIE. Ta wartość ustawia poziom rozliczania zadania na *NONE.

- Należy upewnić się, że napisana informacja dotycząca strategii ochrony dla własnego przedsiębiorstwa jest podobna do przykładu przygotowanego przez Sharon Jones i Johna Smitha.
- Należy upewnić się, że dokonane wybory dla wartości systemowych zostały wpisane w Formularzu wybierania wartości systemowych.
- Należy zanotować, co ma być dołączone do wytycznych ochrony.

Po podaniu w Formularzu wybierania wartości systemowych wszystkich opcji i napisaniu strategii ochrony, można zaplanować grupy użytkowników.

Przykład: strategia ochrony dla przedsiębiorstwa JKL Toy: Przedstawione poniżej wytyczne ilustrują strategię ochrony, którą John Smith, prezes przedsiębiorstwa JKL Toy, wysyła do swoich pracowników. Do przygotowania tych wytycznych skorzystał z notatek, które pisał razem z Sharon.

Tabela 18. Przykład: wytyczne ochrony dla przedsiębiorstwa JKL Toy

Od: Johna Smitha, prezesa

Tabela 18. Przykład: wytyczne ochrony dla przedsiębiorstwa JKL Toy (kontynuacja)

JKL Toy Company

Do: Wszyscy pracownicy przedsiębiorstwa JKL Toy Company

Temat: Ochrona nowego systemu

Wszyscy byli obecni na spotkaniu informacyjnym na temat nowego systemu. Ci pracownicy, którzy będą go używać, rozpoczęli szkolenie i zaczną realizować zamówienia klientów w przyszłym tygodniu. Przewidujemy, że ten system szybko stanie się główną przyczyną sukcesów naszego przedsiębiorstwa.

Chciałbym przedstawić nasze decyzje i strategię ochrony oraz zwrócić uwagę na ich ważność. Te strategie zostały utworzone w celu zabezpieczenia informacji, które są krytyczne dla naszej firmy.

- Za ochronę nowego systemu odpowiedzialna jest Sharon Jones. Będzie jej asystował Ken Harrison. Jeśli są jakieś pytania lub wątpliwości związane z jakimikolwiek problemami dotyczącymi ochrony, należy się kontaktować z nimi.
- Decyzje dotyczące tego, kto może wykonywać funkcje w systemie, zostały oparte na bieżącej strategii dotyczącej informacji. Na przykład:
  - kontrakty i wycena specjalna to informacje, które są poufne; nigdy nie mogą być ujawniane osobom z zewnątrz,
  - tylko księgowość może ustawiać i zmieniać limity kredytowe dla naszych klientów.
- Każdy, kto musi korzystać z systemu, otrzyma identyfikator użytkownika i hasło. System zażąda zmiany hasła po pierwszym wpisaniu się oraz po każdych 60 dniach. Należy wybrać hasło, które można zapamiętać, ale nie takie, które jest oczywiste. Przekazany formularz z identyfikatorem użytkownika zawiera kilka sugestii dotyczących tworzenia haseł.
- *Nie współużytkujcie swojego hasła z nikim*. Naszym zamiarem było umożliwienie wam wykonywania w systemie wszystkich zadań niezbędnych podczas wykonywania codziennych obowiązków.Jeśli potrzebny jest dostęp do innych informacji, skontaktujcie się z Sharon lub Kenem. Jeśli zapomnicie swojego hasła, Sharon lub Ken natychmiast mogą ustawić nowe. Dlatego nie ma żadnego powodu, aby wpisywać się za pomocą identyfikatora i hasła kogoś innego.
- Wiecie, w jaki sposób korzystać z funkcji zapisywania i odtwarzania na stacji roboczej, w celu oszczędzenia pisania. *Nie* używajcie tej funkcji do zapisywania hasła.
- Nie zostawiajcie swoich stacji roboczych z wpisanym identyfikatorem i hasłem, gdy odchodzicie od swojego biurka. Na szkoleniu pokazano, jak tymczasowo wypisywać się ze stacji roboczej. Korzystajcie z tej funkcji w przypadku odchodzenia od biurka na krótki okres czasu. Jeśli odchodzicie na dłużej, zakończcie swoją pracę i wypiszcie się z systemu.

  Wypisywanie się przy odchodzeniu od stacji roboczej jest szczególnie ważne w miejscach, do których jest dostęp publiczny, takich jak rampa załadowcza, pokój obsługi klienta lub zdalne biura sprzedaży.
- Mimo że jednostka systemowa jest bardzo solidna, proszę unikać uderzania w nią lub umieszczania na niej różnych rzeczy. Panele sterujące jednostki będą wyłączone, ale proszę ich nie dotykać. Pracownicy księgowości są odpowiedzialni za to, żeby nikt nie majstrował przy jednostce systemowej.

Pamiętajcie, nasz nowy system ma ułatwić wykonywanie wszystkich zadań oraz poprawić wydajność przedsiębiorstwa. Strategie ochrony powinny pomagać, a nie przeszkadzać. Jeśli są jakieś pytania lub uwagi, nie należy się wahać i skontaktować z Sharon, Kenem lub ze mną.

Po utworzeniu szkicu strategii ochrony można rozpocząć planowanie grup użytkowników.

Planowanie grup użytkowników

Pierwszy krok w procesie planowania, decydowanie o strategii ochrony, jest podobny do ustawiania strategii dla przedsiębiorstwa. Teraz użytkownik jest gotów do planowania grup użytkowników, co jest podobne do decydowania o strategii działu.

Co to jest grupa użytkowników?

Grupa użytkowników jest dokładnie tym, na co wskazuje nazwa: grupą osób, które wymagają tych samych aplikacji i korzystają z nich w ten sam sposób. Zazwyczaj grupa użytkowników składa się z osób pracujących w tym samym dziale i mających podobne zadania. Grupa użytkowników definiowana jest przez tworzenie profilu grupowego.

Co robi profil grupowy?

Profil grupowy spełnia w systemie dwie role:

- **narzędzia ochrony**: profil grupowy udostępnia prosty sposób organizowania, kto ma dostęp od pewnych obiektów w systemie (uprawnienia dla obiektu); zamiast definiowania uprawnień do obiektów dla pojedynczych członków grupy, można zdefiniować je dla całej grupy,
- **narzędzia dostosowywującego**: profil grupowy można wykorzystać jako wzorzec do tworzenia pojedynczych profili użytkowników; większość osób należących do tej samej grupy ma takie same potrzeby konfiguracyjne, takie jak menu początkowe oraz domyślna drukarka; te elementy można zdefiniować w profilu grupowym, a następnie skopiować je do pojedynczych profili użytkowników.

Profile grupowe ułatwiają obsługę prostego, spójnego schematu ochrony oraz dostosowywania.

Które formularze są potrzebne?

Aby zaplanować grupy użytkowników, potrzebne są następujące formularze:

- Formularz identyfikowania grupy użytkowników
- Formularz opisywania grupy użytkowników

Uwaga: Dla każdej grupy użytkowników potrzebny będzie jeden Formularz opisywania grupy użytkowników.

W celu uzyskania pomocy przy wypełnianiu tych formularzy, należy przejrzeć poniższe tematy:

- Identyfikowanie grup użytkowników
- Planowanie profili grupowych
- Wybieranie wartości systemowych, które wpływają na wpisywanie się
- Wybieranie wartości systemowych, które ograniczają możliwości użytkowników
- Wybieranie wartości systemowych, które konfigurują środowisko użytkownika.

Identyfikowanie grup użytkowników

Po zaplanowaniu grup użytkowników, najpierw należy zidentyfikować grupy użytkowników w systemie. Umożliwi to zaplanowanie dostępu do zasobów, którego wymagają te grupy. Należy używać prostej metody identyfikowania grup użytkowników. Należy zwrócić uwagę na działy lub grupy robocze, które planują korzystać z systemu. Należy także kierować się diagramem aplikacji, który został wcześniej narysowany. Trzeba także sprawdzić, czy istnieją naturalne relacje między grupami roboczymi a aplikacjami:

- Czy dla każdej grupy roboczej można zidentyfikować podstawową aplikację?
- Czy wiadomo, jakiej aplikacji potrzebuje każda grupa? Jakich aplikacji nie potrzebują?
- Czy wiadomo, która grupa powinna mieć prawo własności do informacji w każdej bibliotece aplikacji?

Jeśli odpowiedź na te pytania brzmi ″Tak″, to można rozpocząć planowanie grup użytkowników. Jednak jeśli odpowiedziano ″czasami″ lub ″może″, wtedy należy skorzystać z systematycznego podejścia pomagającego w identyfikowaniu grup użytkowników.

Można zapoznać się z przykładem korzystania z tego podejścia do.

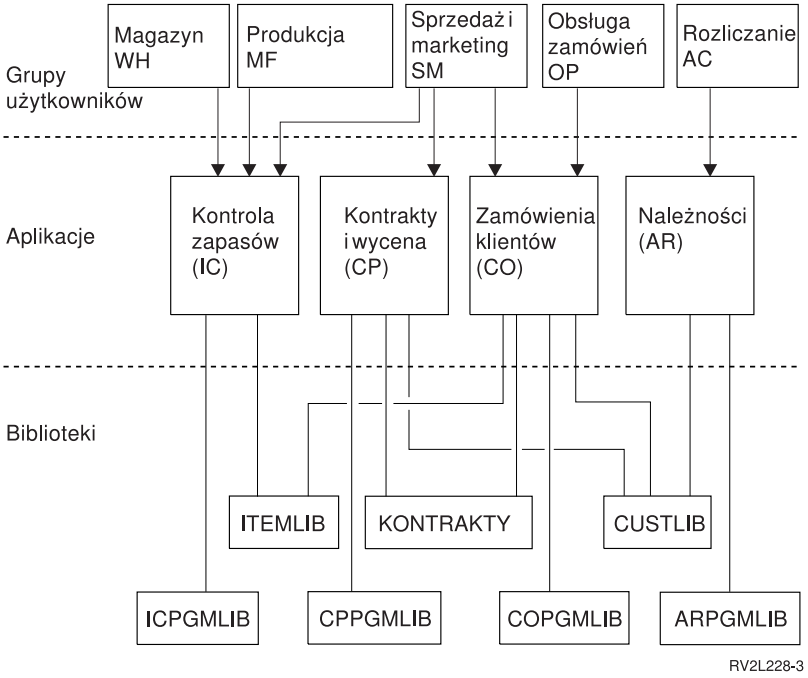
Uwaga: Przypisanie użytkowników tylko do jednego profilu grupowego upraszcza zarządzanie ochroną. Jednak w niektórych sytuacjach można zyskać przypisując użytkowników do więcej niż jednego profilu grupowego.

Przypisanie użytkowników do więcej niż jednego profilu grupowego jest łatwiejsze w zarządzaniu niż nadawanie wielu prywatnych uprawnień pojedynczym profilom użytkowników.

Przykład: identyfikowanie grup użytkowników: Jeśli powiązania między grupami roboczymi i aplikacjami wydają się skomplikowane i niejasne, zastosowanie techniki macierzy, takiej jak Formularz identyfikowania grupy użytkowników, może wyjaśnić niektóre sprawy. Podczas rysowania na macierzy użytkowników systemu i potrzebnych

im aplikacji warto korzystać z wzorca. Oprócz wypełnienia Formularza identyfikowania grupy użytkowników w celu zidentyfikowania, które grupy użytkowników wymagają dostępu do aplikacji, Sharon Jones wykorzystała diagram aplikacji.

Przedstawiony poniżej rysunek ilustruje diagram aplikacji dla przedsiębiorstwa JKL Toy.



Jeśli podejście do ochrony jest łagodne, aby wskazać, że użytkownik wymaga aplikacji, należy użyć znaku X. Jeśli podejście do ochrony jest ścisłe, należy rozważyć, w jaki sposób użytkownicy korzystają z aplikacji. Jeśli ktoś potrzebuje tylko przeglądać informacje aplikacji, zamiast znaku X, w macierzy należy wpisać literę P (przeglądanie). Litera Z (zmiana) oznacza, że ktoś musi wprowadzać zmiany w informacjach. Litera W (właściciel) oznacza, że ktoś odpowiada za dane informacje.

Na przykład w przedsiębiorstwie JKL Toy wiele grup wymaga dostępu do aplikacji Kontrakty i wycena:

- dział sprzedaży i marketingu ustala ceny i przygotowuje kontrakty z klientami; osoby z tego działu są *właścicielami* informacji na temat cen i kontraktów,
- dział zamówień klientów pośrednio zmienia informacje w kontraktach; kiedy osoby z tego działu obsługują zamówienia, w kontraktach zmienia się ilość; potrzebują oni *zmieniać* informacje na temat cen i kontraktów,
- osoby obsługujące zamówienia planując swoją pracę muszą znać informacje na temat limitów kredytowych, ale nie mogą ich zmieniać; potrzebują oni *przeglądać* informacje o limitach kredytowych.

Tabela 19. Formularz identyfikowania grupy użytkowników dla przedsiębiorstwa JKL Toy: przykład

Formularz identyfikowania grupy użytkowników					
Przygotowany przez: Sharon Jones		Data: 9/2/99			
		Wymagany dostęp do aplikacji			
Nazwa użytkownika	Dział	APP: CO	APP: IC	APP: PC	APP: AR
Ken H.	Obsługa zamówień (OP)	W	Z	Z	Z
Karen R.	Obsługa zamówień (OP)	W	Z	Z	Z
Kris T.	Księgowość (AC)	P		P	W
Sandy J.	Księgowość (AC)	P	Z	P	W

Tabela 19. Formularz identyfikowania grupy użytkowników dla przedsiębiorstwa JKL Toy: przykład (kontynuacja)

Peter D.	Księgowość (AC)	Z		P	W
Ray W.	Magazyn (WH)	P	W	P	
Rose Q.	Magazyn (WH)	P	W	P	
Roger T.	Sprzedaż i marketing (SM)	Z	Z	W	Z
Sharon J.	Menedżerowie (MG)	Z	Z	Z	Z

Uwaga:

- W przypadku *łagodnego* środowiska ochrony, aby zaznaczyć wymagane przez użytkowników aplikacje, należy użyć znaku X.
- W przypadku *średniego* środowiska ochrony, aby zaznaczyć którzy użytkownicy będą mieli uprawnienia do danej aplikacji, należy użyć litery A.
- W przypadku *ścisłego* środowiska ochrony, aby określić w *jaki* sposób aplikacja jest wymagana, należy użyć litery Z (zmiana), P (przeglądanie) i W (właściciel).

Podczas przygotowywania macierzy, Sharon Jones zrobiła kilka notatek:

- obsługa zamówień i księgowość dostarczają sobie wzajemnie informacje; obecnie wymagają podobnych aplikacji; jednak powinny to być oddzielne grupy, ponieważ w przyszłości, w miarę dodawania nowych osób działy będą bardziej wyspecjalizowane,
- chociaż obsługa zamówień nie może bezpośrednio zmieniać zapasów lub kontraktów, to artykuły i salda kontraktów zmieniają się automatycznie w momencie tworzenia i realizowania zamówień; czy później stanie się to zagadnieniem dotyczącym ochrony?
- osoby z działu sprzedaży i marketingu związane są ze wszystkimi częściami przedsiębiorstwa oraz wszystkimi aplikacjami; ustalają ceny oraz opisy artykułów; konfigurują nowych klientów, chociaż to księgowość ustawia limity kredytowe; odpowiedzialni są za ustalanie wszystkich terminów i cen kontraktów.

Należy zadecydować, czym powinna być dana grupa. Jeśli do tego potrzebna jest pomoc, należy wypełnić Formularz identyfikowania grupy użytkowników.

Po dodaniu użytkowników do Formularza identyfikowania grupy użytkowników, można zaplanować profil grupowy.

Planowanie profilu grupowego

Po zidentyfikowaniu grup użytkowników, można zaplanować profil dla każdej grupy. Wiele z podjętych decyzji wpłynie zarówno na ochronę jak i na konfigurację. Na przykład po określeniu menu początkowego można ograniczyć dostęp użytkowników tylko do tego menu. Ale można także zapewnić, że użytkownik zobaczy poprawne menu po wpisaniu się.

Należy przygotować Formularz opisywania grupy użytkowników dla jednej grupy użytkowników. Po wypełnieniu pierwszego formularza należy wrócić do tego miejsca i wypełnić formularze dla pozostałych grup.

Ochrona i konfiguracja systemu iSeries jest bardzo elastyczna. Metoda planowania przedstawiona w tym temacie udostępnia dobry sposób projektowania profili grupowych oraz opisów zadania, ale programista lub dostawca aplikacji może zalecać inną metodę.

Nazywanie profili grupowych

Ponieważ profile grupowe działają jako specjalne rodzaje profilu użytkownika, można je identyfikować, aby łatwo je było wyświetlać lub tworzyć ich listę. Należy przypisać im specjalne nazwy. Aby profile grupowe pojawiały się razem na listach, należy nadać im nazwy rozpoczynające się od takich samych znaków, na przykład GRP (od grupy) lub WYD (od działu). Podczas nadawania nazw grupom użytkowników należy skorzystać z następujących wskazówek:

- nazwy grup użytkowników mogą mieć do 10 znaków,
- nazwa może zawierać litery, cyfry oraz znaki specjalne: funt (#), dolar ($), podkreślenie (_) i znak at (@),
- nazwa nie może rozpoczynać się od cyfry.

Uwaga: Do każdego profilu grupowego system przypisuje numer identyfikacyjny grupy (*gid*). Zazwyczaj generowanie identyfikatora *gid* można pozostawić systemowi. Jeśli system używany jest w sieci, profilom grupowym należy przypisać określony identyfikator gid. Z pomocą administratora sieci można sprawdzić, czy należy przypisywać identyfikatory gid.

System nazewnictwa dla profili grupowych należy dodać do odpowiedniego pola w Formularzu konwencji nazewnictwa. Na przykład Sharon Jones, jako konwencję nazewnictwa dla profili grupowych wybrała WYD. Wpisała ją w odpowiedniej sekcji Formularza konwencji nazewnictwa.

Tabela 20. Formularz Konwencji nazewnictwa dla przedsiębiorstwa JKL Toy: przykład profilu grupowego

Typ obiektu	Konwencja nazewnictwa
Profile grupowe	Należy używać znaków WYD, po których następuje nazwa skrócona działu. Opisem tekstowym profilu grupowego powinna być nazwa działu.

Określanie, jakich aplikacji i bibliotek wymaga grupa użytkowników

Jeśli jeszcze tego nie zrobiono, do diagramu aplikacji i bibliotek który został wcześniej narysowany, należy dodać grupy użytkowników. Ten obraz pomoże przy decydowaniu, których zasobów i aplikacji wymaga każda grupa.

W części 1 Formularza opisywania grupy użytkowników należy wskazać podstawową aplikację grupy, którą jest najczęściej używana aplikacja. Należy podać także pozostałe aplikacje.

Teraz należy spojrzeć na Formularz opisywania aplikacji oraz diagram aplikacji, aby sprawdzić, które biblioteki są wymagane przez grupę. Z pomocą programisty lub dostawcy aplikacji należy ustalić najlepszą metodę udostępniania tych bibliotek. Większość aplikacji korzysta z następujących technik:

- aplikacja dołącza biblioteki do początkowej listy bibliotek użytkownika,
- aplikacja uruchamia program konfiguracyjny, który umieszcza biblioteki na liście bibliotek użytkownika,
- biblioteki nie muszą znajdować się na liście bibliotek; aplikacje zawsze określają bibliotekę.

System korzysta z listy bibliotek podczas wyszukiwania plików i programów potrzebnych do uruchamiania aplikacji. **Lista bibliotek** jest listą bibliotek, którą przeszukuje system, gdy użytkownik potrzebuje obiektów. Ma ona dwie części:

1. **Część systemową**: określoną w wartości systemowej QSYSLIBL, która jest wykorzystywana dla bibliotek systemu OS/400. Wartość domyślna tej wartości systemowej nie musi być zmieniana.
2. **Część użytkownika**: wartość systemowa QUSRLIBL udostępnia część listy bibliotek dla użytkownika. Opis zadania użytkownika zawiera początkową listę bibliotek lub komend dostępnych po wpisaniu się użytkownika. Jeśli w użyciu jest początkowa lista bibliotek, wartość systemowa QUSRLIBL jest nadpisywana. Biblioteki aplikacji powinny być dołączone do części listy bibliotek dla użytkownika.

Korzystanie z opisu zadania

Kiedy użytkownik wpisuje się do systemu, opis zadania użytkownika definiuje wiele charakterystyk dla zadania, które obejmują sposób jego drukowania, sposób uruchamiania zadań wsadowych oraz początkową listę bibliotek. System dostarczany jest z opisem zadania nazywanym QDFTJOBD, którego można użyć do tworzenia profili grupowych. Jednak zadanie QDFTJOBD jako początkową listę bibliotek określa wartość systemową QUSRLIBL. Jeśli różne grupy użytkowników mają mieć dostęp do różnych bibliotek, dla każdej grupy należy utworzyć unikalne opisy zadania.

W Formularzu opisywania grupy użytkowników należy wymienić wszystkie biblioteki, dostępu do których wymaga grupa. Jeśli biblioteka powinna być dołączona do początkowej listy bibliotek w opisie zadania grupy, na formularzu należy wpisać jej nazwę.

Przed rozpoczęciem wybierania wartości systemowych, które wpływają na wpisywanie się, można przejrzeć przykład pokazujący, jak Sharon Jones opisała grupy użytkowników w przedsiębiorstwie JKL Toy.

Przykład: Formularz opisywania grupy użytkowników dla przedsiębiorstwa JKL Toy: Pierwsza tabela prezentuje część 1 Formularza opisywania grupy użytkowników, który Sharon Jones przygotowała dla działu sprzedaży i marketingu. Należy zauważyć, że do początkowej listy bibliotek nie dołączyła bibliotek KONTRAKTY i CPPGMLIB. Aplikacja dodaje je do listy bibliotek automatycznie, nie trzeba ich dodawaćdo początkowej listy bibliotek DPTSM. Kiedy użytkownicy skończą aplikację, system usuwa te biblioteki z listy. Zapewnia to dodatkową ochronę tych bibliotek, ponieważ dostępne są tylko przez aplikację.

Tabela 21. Formularz opisywania grupy użytkowników dla przedsiębiorstwa JKL Toy: przykład informacji opisowych

Formularz opisywania grupy użytkowników	Część 1 z 2
Przygotowany przez: Sharon Jones	Data: 9/5/99
Nazwa profilu grupowego: DPTSM Opis grupy: dział sprzedaży i marketingu	
Podstawowa aplikacja dla grupy: Kontrakty u wycena Pozostałe aplikacje wymagane przez grupę: Zapasy (do wprowadzania opisów produktów i cen), Zamówienia klientów	
Biblioteki wymagane przez grupę. Zaznacz (✓) każdą bibliotekę, która powinna znaleźć się na początkowej liście bibliotek dla tej grupy: • ✓CUSTLIB • ✓ITEMLIB • ✓COPGMLIB • ✓ICPGMLIB • CPPGMLIB • KONTRAKTY	

Dodatkowo Sharon zaczęła wypełniać Formularz opisywania grupy użytkowników dla magazynu.

Tabela 22. Formularz opisywania grupy użytkowników: informacje opisowe

Formularz opisywania grupy użytkowników	Część 1 z 2
Przygotowany przez: Sharon Jones	Data: 9/5/99
Nazwa profilu grupowego: DPTWH Opis grupy: magazyn	
Podstawowa aplikacja dla grupy: Kontrola zapasów Pozostałe aplikacje wymagane przez grupę: brak	
Biblioteki wymagane przez grupę. Zaznacz (✓) każdą bibliotekę, która powinna znaleźć się na początkowej liście bibliotek dla tej grupy: • ✓ITEMLIB • ✓ICPGMLIB.	

Po wypełnieniu części 1 Formularza opisywania grupy użytkowników, można rozpocząć wybieranie wartości, które wpływają na wpisywanie się.

Wybieranie wartości, które wpływają na wpisywanie się

Po zaplanowaniu profili grup, należy wybrać wartości systemowe, które wpływają na wpisywanie się. Wybór należy wpisać w części 2 Formularza opisywania grupy użytkowników. Należy pamiętać, że wybrane wartości zostaną skopiowane w celu utworzenia pojedynczych profili członków grupy. Należy zacząć od wpisania wybranej nazwy profilu grupowego oraz krótkiego opisu (tekstu) dla grupy.

Jeśli system jest konfigurowany prawidłowo, użytkownicy muszą podawać na ekranie wpisywania się jedynie swoje identyfikatory oraz hasła. Profile użytkowników udostępniają pozostałe wartości wpisywania się.

Hasło

Dla profilu grupowego hasło powinno mieć wartość *NONE. Zapobiegnie to wpisywaniu się za pomocą profilu grupowego. Później, po skopiowaniu profilu w celu utworzenia pojedynczych profili użytkowników, dla każdego użytkownika należy utworzyć hasło.

Program i procedura początkowa

Program początkowy użytkownika, często nazywany **programem wpisywania się**, jest uruchamiany zanim system wyświetli pierwsze menu. W profilu grupowym należy podać zarówno nazwę programu, jak i bibliotekę, nawet jeśli biblioteka jest częścią początkowej listy bibliotek. Podając oba parametry zyskujemy pewność, że system uruchomi poprawny program oraz nie trzeba się martwić o zmiany listy bibliotek.

Program lub procedura początkowa używane są z następujących powodów:

- niektóre aplikacje korzystają z programów początkowych do skonfigurowania środowiska aplikacji,
- chcemy, aby użytkownik uruchamiał tylko jeden program i nigdy nie widział menu; na przykład w przedsiębiorstwie JKL Toy, osoby które korzystają ze stacji roboczych na rampie załadowczej mogą uruchamiać tylko program do pobierania zapasów; zmniejsza to ryzyko naruszenia ochrony na stacjach roboczych dostępnych w miejscach publicznych.

Ustawienie wartości *YES lub *PARTIAL w polu **Ograniczenie możliwości** zapobiega zmianie programu początkowego przez użytkownika.

Z pomocą programisty należy sprawdzić, czy aplikacje wymagają programu lub procedury początkowej.

Menu początkowe oraz biblioteka menu początkowego

Menu początkowe, nazywane także **pierwszym menu**, jest pierwszym menu, które widzi użytkownik po wpisaniu się. Program początkowy uruchamia się przed pojawieniem się menu początkowego. Jeśli program początkowy wyświetla jakieś ekrany, użytkownik zobaczy je, zanim system wyświetli menu początkowe.

Zazwyczaj menu początkowe dla grupy powinno być menu podstawowym głównej aplikacji grupy. Należy podać nazwę menu oraz jego bibliotekę.

Ustawienie wartości *YES w polu **Ograniczenie możliwości**, uniemożliwia użytkownikowi zmianę menu początkowego. Ustawienie wartości *PARTIAL w polu *Ograniczenie możliwości*, umożliwia użytkownikowi zmianę menu początkowego.

Biblioteka bieżąca

Biblioteka bieżąca nazywana jest także **biblioteką domyślną**. Jeśli dla użytkownika określona zostanie biblioteka bieżąca, może zdarzyć się kilka rzeczy:

- jeśli użytkownik tworzy obiekty, takie jak zapytania, system umieszcza te obiekty w bibliotece bieżącej, chyba że użytkownik określił inną bibliotekę,
- system automatycznie dodaje bibliotekę bieżącą do części listy bibliotek dla użytkownika; Biblioteka bieżąca może, ale nie musi być dołączona do początkowej listy bibliotek w opisie zadania,
- biblioteka bieżąca staje się pierwszą biblioteką w części listy bibliotek dla użytkownika; przed przeszukaniem bibliotek na liście bibliotek użytkownika, w poszukiwaniu plików i programów system przeszukuje bibliotekę bieżącą,
- jeśli użytkownik nie ma przypisanej biblioteki bieżącej, system przypisuje mu bibliotekę QGPL (ogólnego przeznaczenia).

Zalecenia

Biblioteka bieżąca jest szczególnie ważna w przypadku planowania wykorzystania programu licencjonowanego IBM Query for iSeries lub innego podobnego programu. Należy skorzystać z jednego z następujących podejść:

- dla każdej w grupy należy utworzyć bibliotekę współużytkowaną; wszystkie zapytania oraz pliki i zbiory dla grupy należy umieścić w tej bibliotece; należy nadać jej taką samą nazwę,jak nazwa profilu grupowego, i wpisać ją jako bieżącą bibliotekę dla grupy,
- każdemu użytkownikowi, który będzie korzystał z programu Query, należy przydzielić bibliotekę osobistą; należy nadać jej taką samą nazwę, jak nazwa profilu użytkownika; należy także określić, że jest to biblioteka bieżąca indywidualnych profili członków grupy, a nie profilu grupowego.

W części 2 Formularza opisywania użytkowników w polach dotyczących wpisywania się należy wpisać dokonane wybory.

Po wybraniu wartości, które wpływają na wpisywanie się, można wybrać wartości, które ograniczają działania użytkowników.

Wybieranie wartości ograniczających działanie użytkowników

Po wpisaniu w części 2 Formularza opisywania grupy użytkowników wyborów dotyczących wartości wpływających na wpisywanie się, należy rozważyć ograniczenie działań użytkowników w systemie. Działania użytkowników można ograniczyć z następujących powodów:

- aby zapobiec korzystaniu z komend CL; mogą one kusić do eksperymentowania i spowodować nieumyślne uszkodzenie pewnych elementów,
- aby ograniczyć użytkownikom określone aplikacje i funkcje,
- aby udostępnić proste środowisko, w którym użytkownicy nie będą musieli dokonywać niepotrzebnych wyborów.

Na to, co może zrobić użytkownik, wpływ ma wiele czynników:

- projekt aplikacji,
- wartości systemowe,
- ochrona zasobów,
- profile grupowe,
- profile użytkowników,
- opisy zadań.

Pola **Ograniczenie możliwości** oraz **Klasa użytkownika** w profilu grupowym lub użytkownika określają, które decyzje administratora użytkownik może przesłonić.

Ograniczenie możliwości

Pole **Ograniczenie możliwości** nazywane jest **Ograniczonym wierszem komend**. Można zdecydować, czy użytkownicy mogą zmieniać wartości na ekranie wpisywania się, wprowadzać komendy oraz zmieniać swoje programy obsługi klawisza ATTN. Można wybrać ścisłe ograniczenie (*YES), średnie (*PARTIAL) lub brak ograniczeń (*NO). Przedstawiona poniżej tabela pokazuje, co umożliwiają te wartości:

Tabela 23. Funkcje dozwolone dla danej wartości ograniczenia możliwości

Wartość ograniczenia możliwości	Zmiana programu początkowego	Zmiana menu początkowego	Zmiana bieżącej biblioteki	Zmiana programu klawisza ATTN	Wprowadzanie komend
*YES	Nie	Nie	Nie	Nie	Częściowo[1]
*PARTIAL	Nie	Tak	Nie	Nie	Tak
*NO	Tak	Tak	Tak	Tak	Tak

1 Dozwolone są komendy: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG i STRPCO. Użytkownik nie może używać klawisza F9 służącego do wyświetlania wiersza komend z dowolnego menu Asysty Operacyjnej lub ekranu.

Klasa użytkownika

Klasa użytkownika, zwana również **typem użytkownika**, określa które opcje Asysty Operacyjnej i menu systemowych widzi użytkownik. Określa także, które funkcje systemowe może wykonywać użytkownik, chyba że w polu **Uprawnienia specjalne** ma podaną listę uprawnień.

Zalecenia dotyczące ograniczonych możliwości i klasy użytkownika

Większość użytkowników może nie potrzebować lub nie chcieć dostępu do komend CL i funkcji systemowych. Ekrany Asysty Operacyjnej przekazują użytkownikowi wystarczającą ilość informacji oraz umożliwiają wystarczającą kontrolę nad ich pracą. Poniższe zalecenia umożliwiają użytkownikom dostęp tylko do tych zasobów systemu, które są im potrzebne do wykonywania zadań:

- w każdym profilu grupowym, pole **Ograniczenie możliwości** należy ustawić na wartość *YES; *Klasę użytkownika* na *USER,
- powyższą specyfikację należy przesłonić w przypadku pojedynczych użytkowników, którzy potrzebują dostępu do funkcji systemowych,
- jeśli trzeba, należy upewnić się, że menu umożliwiają przemieszczanie się między aplikacjami.

Po wpisaniu w części 2 Formularza opisywania grupy użytkowników wybranych wartości pól Klasa użytkownika i Ograniczenie możliwości, można wybrać wartości, które konfigurują środowisko użytkownika.

Wybieranie wartości systemowych, które konfigurują środowisko użytkownika.

Po podaniu w części 2 Formularza opisywania grupy użytkowników wyborów dotyczących ograniczania działania użytkowników w systemie, można wybrać wartości, które określają środowisko operacyjne użytkownika. Środowisko operacyjne użytkownika określa wiele pól jego profilu. Są to drukarki, których może używać, kolejka, do której mają być wysyłane komunikaty, informacja, z jakim priorytetem powinny być uruchamiane zadania. Dla wielu z tych pól zalecane są ustawienia domyślne. W poniższych paragrafach opisano kilka pól.

- **Opis zadania oraz biblioteka opisu zadania**: te pola informują system, jakiego opisu zadania należy użyć podczas wpisywania się użytkownika. Opis zadania zawiera początkową listę bibliotek. Nazwa opisu zadania każdej grupy użytkowników powinna być taka sama, jak nazwa profilu grupowego. Opisy zadań zazwyczaj umieszczane są w bibliotece QGPL.
- **Drukarka i kolejka wyjściowa**: wydruki tworzone przez użytkownika przesyłane są do drukarki z listy jego profilu, chyba że określone zadanie drukowania wysyła je do innej drukarki. Członkowie grupy użytkowników zazwyczaj ulokowani są w tym samym miejscu i współużytkują tę samą drukarkę. Drukarkę można przypisać w profilu grupowym i skopiować ją do każdego pojedynczego profilu użytkownika. Drukarka użytkownika nazywana jest także **drukarką domyślną**.

  Kolejka wyjściowa przechowuje wydruki, przed ich wydrukowaniem. Zazwyczaj każda drukarka ma własną kolejkę wyjściową o tej samej nazwie. Aby system korzystał z kolejki wyjściowej drukarki, dla kolejki wyjściowej należy podać parametr *DEV.

  W Formularzu opisywania grupy użytkowników należy wpisać nazwę opisu zadania, jego bibliotekę oraz drukarkę domyślną.
- **Konfigurowanie interfejsu Asysty Operacyjnej**: kiedy dostarczany jest nowy system, menu Asysty Operacyjnej dla każdego użytkownika jest program obsługi klawisza ATTN. Jeśli użytkownik naciśnie klawisz ATTN, zobaczy menu Asysty Operacyjnej (ASSIST). Jeśli aplikacja korzysta z innego programu obsługi klawisza ATTN, użytkownikom należy udostępnić inną metodę dostępu do menu Asysty Operacyjnej:
  - za pomocą poleceń GO ASSIST lub CALL QEZAST, do menu aplikacji głównej należy dodać opcję dostępu do menu Asysty Operacyjnej,
  - nakazać użytkownikom wpisanie w wierszu komend polecenia GO ASSIST.

Jeśli w profilu użytkownika pole **Ograniczenie możliwości** ma wartość *YES, użytkownik nie będzie mógł skorzystać z komendy GO, aby wyświetlić menu. Należy wtedy udostępnić użytkownikom Asysty Operacyjnej inną metodę dostępu do menu ASSIST.

Można zapoznać się z przykładem, w którym przedstawiono Formularz opisywania grupy użytkowników dla przedsiębiorstwa JKL Toy z wybranymi przez Sharon Jones wartościami.

Aby zakończyć powyższe czynności dotyczące planowania, należy:

- dla każdej grupy użytkowników w przedsiębiorstwie wypełnić Formularz opisywania grupy użytkowników,
- w Formularzu konwencji nazewnictwa opisać w jaki sposób nazywane są grupy użytkowników,
- do diagramu aplikacji i bibliotek dodać grupy użytkowników.

Po wykonaniu tych czynności, można rozpocząć planowanie pojedynczych profili użytkowników.

Przykład: Formularz opisywania grupy użytkowników dla przedsiębiorstwa JKL Toy — część 2: Sharon Jones podczas przygotowywania Formularza opisywania grupy użytkowników dla personelu sprzedaży i marketingu, zrobiła kilka notatek o tym dziale oraz o magazynie.

- Personel sprzedaży i marketingu często będzie korzystał z programu IBM Query for iSeries. Każdy użytkownik powinien mieć prywatną bibliotekę. Magazyn może mieć jedną bibliotekę grupową.
- Osoby z magazynu, które pracują na rampie załadowczej, zamiast menu początkowego potrzebują programu początkowego.

Część 2 Formularza opisywania grupy użytkowników, który Sharon przygotowała dla dwóch działów.

Tabela 24. Formularz opisywania grupy użytkowników dla przedsiębiorstwa JKL Toy: przykład działu Sprzedaży i marketingu

Nazwa pola	Zalecana wartość	Wybór użytkownika
Nazwa profilu grupowego (użytkownik)		DSTSM
Hasło	*NONE	*NONE
Klasa użytkownika (Rodzaj użytkownika)	*USER	*USER
Biblioteka bieżąca (Biblioteka domyślna)	*taki sam jak nazwa profilu grupowego*	(w przypadku grupy pole ma być puste; wypełnić dla pojedynczych profili)
Wywoływany program początkowy (program wpisywania się)		
Biblioteka programu początkowego		
Menu początkowe (pierwsze menu)		CPMAIN
Biblioteka menu początkowego		CPMAINLIB
Ograniczenie możliwości (ograniczenie użycia wiersza komend)	*YES	*PARTIAL
Tekst (opis użytkownika)		Sprzedaż i marketing
Opis zadania	*taki sam jak nazwa profilu grupowego*	DPTSM
Biblioteka opisu zadania		QGPL
Nazwa profilu grupowego (grupa użytkowników)	*NONE[1]	*NONE
Drukarka (drukarka domyślna)		PRT03
Kolejka wyjściowa	*DEV	*DEV

Tabela 25. Formularz opisywania grupy użytkowników dla przedsiębiorstwa JKL Toy: przykład magazynu

Nazwa pola	Zalecana wartość	Wybór użytkownika
Nazwa profilu grupowego (użytkownik)		DPTWH
Hasło	*NONE	*NONE

Tabela 25. Formularz opisywania grupy użytkowników dla przedsiębiorstwa JKL Toy: przykład magazynu (kontynuacja)

Nazwa pola	Zalecana wartość	Wybór użytkownika
Klasa użytkownika (Rodzaj użytkownika)	*USER	*USER
Środowisko specjalne		
Biblioteka bieżąca (Biblioteka domyślna)	*taki sam jak nazwa profilu grupowego*	DPTWH
Wywoływany program początkowy (program wpisywania się)		
Biblioteka programu początkowego		
Menu początkowe (pierwsze menu)		ICMAIN
Biblioteka menu początkowego		ICPGMLIB.
Ograniczenie możliwości (ograniczenie użycia wiersza komend)	*YES	*YES
Tekst (opis użytkownika)		Magazyn
Opis zadania	*taki sam jak nazwa profilu grupowego*	DPTWH
Biblioteka opisu zadania		QGPL
Nazwa profilu grupowego (grupa użytkowników)	*NONE[1]	*NONE
Drukarka (drukarka domyślna)		PRT04
Kolejka wyjściowa	*DEV	*DEV

1 W przypadku profilu grupowego nazwa profilu grupowego musi mieć wartość *NONE. Profil grupowy nie może być członkiem innej grupy.

Teraz można rozpocząć planowanie pojedynczych profili użytkowników.

Planowanie pojedynczych profili użytkowników

Po zadecydowaniu o ogólnej strategii ochrony i zaplanowaniu grup użytkowników można zaplanować pojedyncze profile użytkowników.

Które formularze są potrzebne?

Do zaplanowania pojedynczych profili użytkowników należy skorzystać z następujących formularzy:

- Formularz pojedynczego profilu użytkownika
- Formularz odpowiedzialności w systemie

Potrzebne będą także informacje z formularzy:

- Formularz definiowania grupy użytkowników
- Formularz konwencji nazewnictwa
- Diagram aplikacji

Nadawanie nazw profilom użytkowników

Nazwa profilu użytkownika to sposób identyfikacji użytkownika w systemie. Nazwę profilu użytkownika wpisuje się w polu **Identyfikator użytkownika** w oknie wpisywania się. Cała praca oraz tworzone wydruki powiązane są z nazwą danego profilu użytkownika.

Podczas decydowania, jak nazwać profile użytkowników, należy rozważyć następujące kwestie:

- nazwa profilu użytkownika może mieć do 10 znaków; niektóre metody komunikacji ograniczają ją do 8 znaków,
- nazwa profilu użytkownika może zawierać litery, cyfry oraz znaki specjalne: funt (#), dolar ($), podkreślenie (_) i znak at (@); nie może rozpoczynać się od cyfry lub podkreślenia (_),
- system nie rozróżnia wielkich i małych liter w nazwie profilu użytkownika; po wpisaniu małych liter alfabetu, system zamienia je na wielkie litery,
- ekrany i listy wykorzystywane do zarządzania profilami użytkowników wyświetlają je w porządku alfabetycznym, według nazw,
- wszystkie profile dostarczone przez firmę IBM rozpoczynają się od litery Q; aby odróżnić profile tworzone przez użytkownika, należy unikać nadawania im nazw rozpoczynających się od litery Q.

Zalecenia

Jedną z technik nadawania nazwy profilowi użytkownika jest użycie pierwszych 7 znaków nazwiska, z następującym po nich pierwszym znakiem imienia. Poniżej przedstawiono konwencje nazewnictwa, które Sharon wykorzystała dla profili użytkowników przedsiębiorstwa JKL Toy:

Tabela 26. Formularz konwencji nazewnictwa dla przedsiębiorstwa JKL Toy: przykład profilu użytkownika

Nazwa użytkownika	Nazwa profilu użytkownika
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jones, Sharon	JONESS

Ta metoda ułatwia zapamiętanie nazw profili użytkowników. Umożliwia także ustawianie list i ekranów w porządku alfabetycznym, według nazwisk.

Na przykład taką technikę planuje zastosować Sharon Jones z przedsiębiorstwa JKL Toy. Wypełniła odpowiednią sekcję w Formularzu konwencji nazewnictwa.

Tabela 27. Formularz konwencji nazewnictwa dla przedsiębiorstwa JKL Toy: przykład profilu użytkownika

Typ obiektu	Konwencja nazewnictwa
Profile użytkowników	Należy użyć pierwszych 7 znaków nazwiska użytkownika, z następującym po nich pierwszym znakiem imienia. Opisem profilu użytkownika będzie nazwisko, imię.

W Formularzu konwencji nazewnictwa należy opisać sposób nadawania nazw profilom użytkowników, a następnie można określić, kto powinien być odpowiedzialny za funkcje systemowe oraz wybrać wartości dla każdego użytkownika.

Określanie, kto powinien być odpowiedzialny za funkcje systemu

Podczas planowania pojedynczych profili użytkowników najpierw należy określić odpowiedzialność użytkowników w systemie. Aby system mógł działać wydajnie, użytkownicy muszą regularnie wykonywać funkcje zarządzające i konserwacyjne. Osoby wykonujące takie zadania wymagają uprawnień do uruchamiania komend i wykonywania funkcji systemowych.

W sekcji Wybieranie wartości ograniczających działanie użytkowników omówiono, w jaki sposób pola **Klasa użytkownika** i **Ograniczenie możliwości** kontrolują funkcje systemowe, do których mają dostęp użytkownicy. Zazwyczaj większości użytkowników należy uniemożliwić wykonywanie funkcji systemowych (Klasa użytkownika powinna mieć wartość *USER, a Ograniczenie możliwości - *PARTIAL lub *YES). Jednak niektórzy użytkownicy wymagają dodatkowych uprawnień do utrzymania wydajności systemu na wymaganym poziomie.

Przedstawiona poniżej tabela zawiera listę niektórych ważnych zadań dotyczących zarządzania systemem. Wskazuje także na klasę użytkownika oraz uprawnienia specjalne, które można przypisać użytkownikom odpowiedzialnym za nie. Ta lista pomaga w określaniu, którzy użytkownicy systemu wymagają uprawnień specjalnych. Jednak nie jest to

pełne narzędzie do planowania działania i konserwacji systemu. Ta tabela zawiera klasę użytkownika i uprawnienia specjalne, które działają dla większości systemów. Jednak w konkretnym systemie, konieczne może być przypisanie innych uprawnień.

W momencie nadania profilowi klasy użytkownika innej niż *USER, użytkownik automatycznie otrzymuje pewien zestaw uprawnień, który umożliwia wykonywanie funkcji systemowych. Możliwe jest przypisanie uprawnień specjalnych użytkownika innych niż te określone w polu klasy użytkownika, jednak zwykle nie jest to konieczne.

Tabela 28. Odpowiedzialność w systemie, Klasa użytkownika i uprawnienia specjalne

Funkcja systemowa [1]	**Opis**	**Wymagana klasa użytkownika [2]**	**Wymagane uprawnienia specjalne [3]**
Operacje systemowe	Zarządzanie wydrukami, odpowiadanie na komunikaty systemowe, monitorowanie zwykłych operacji, przeprowadzanie ładowania programu początkowego (IPL).	*SYSOPR	*JOBCTL
Konserwacja systemu	Wykonywanie funkcji konserwacji systemu, takich jak ustanawianie harmonogramu automatycznego czyszczenia i monitorowanie użycia dysku.	*SYSOPR	*JOBCTL
Składowanie systemu	Regularne składowanie bibliotek aplikacji systemowych oraz informacji o ochronie. Szczegółowe informacje o tych funkcjach, zawiera temat Składowanie i odtwarzanie w Centrum informacyjnym.	*SYSOPR	*SAVSYS
Administrowanie profilami	Dodawanie nowych profili użytkowników, obsługa istniejących profili.	*SECADM	*SECADM
Administrowanie ochroną zasobów	Obsługa uprawnień do obiektów w systemie.	*SECOFR	*ALLOBJ
Konserwacja programów	Stosowanie okresowych poprawek PTF dla bibliotek dostarczanych przez firmę IBM. Dokonywanie zmian w bibliotekach aplikacji.	*SECOFR	*ALLOBJ
Kontrolowanie ochrony	Konfigurowanie funkcji do kontrolowania ochrony. Określanie, które zdarzenia, użytkownicy i obiekty powinny być kontrolowane.		*AUDIT [4]
Konfigurowanie systemu	Dodawanie, zmiana i usuwanie urządzeń z systemu.		*IOSYSCFG[5]

1 Dla użytkowników, którzy są za to odpowiedzialni, w polu Ograniczenie możliwości należy podać wartość *NO.

2 Jest to minimalna wymagana klasa użytkownika. Klasa użytkownika udostępnia uprawnienia do korzystania z komend i opcji menu, które są wymagane dla tej funkcji. W zależności od ochrony zasobów, wymagane są także dodatkowe uprawnienia do obiektu.

3 To szczególne uprawnienie specjalne wymagane jest dla osób odpowiedzialnych za wykonywanieczynności związanych z zadaniami. Klasa użytkownika może dawać dodatkowe uprawnienia specjalne.

4 Uprawnienie specjalne *AUDIT nie ma odpowiadającej mu klasy użytkownika. Klasa użytkownika *SECOFR obejmuje uprawnienie specjalne *AUDIT. Jednak kontroler prawdopodobnie nie będzie wymagał pozostałych możliwości klasy użytkownika *SECOFR. Każdemu pojedynczemu użytkownikowi, którykontroluje system, należy nadać uprawnienia specjalne *AUDIT.

5 Uprawnienie specjalne *IOSYSCFG nie ma odpowiadającej mu klasy użytkownika. Klasa użytkownika *SECOFR obejmuje uprawnienie specjalne *IOSYSCFG. Uprawnienia specjalne *IOSYSCFG należy nadawać tylko tym użytkownikom, którzy wykonują zadania związane z konfigurowaniem systemu. Tacy użytkownicy mogą tworzyć linie, kontrolery i urządzenia lub konfigurować protokół TCP/IP. Jednak użytkownik konfigurujący system może nie potrzebować innych możliwości klasy użytkownika *SECOFR.

Zalecenia

Za pomocą powyższej tabeli można zaplanować, kto powinien wykonywać funkcje systemowe. Minimum to przydzielenie dwóch osób do zarządzania ochroną systemu oraz dwóch do zarządzania operacjami i kopiami zapasowymi.

Formularz odpowiedzialności w systemie można wykorzystać jako narzędzie do zarządzania i kontrolowania systemu. Należy systematycznie analizować zakresy obowiązków wszystkich osób, które mają uprawnienia specjalne oraz sprawdzać, czy są im rzeczywiście niezbędne.

Przed wybraniem wartości dla każdego użytkownika warto zapoznać się z przykładem określania odpowiedzialności użytkowników przez Sharon Jones.

Przykład: Formularz odpowiedzialności w systemie dla przedsiębiorstwa JKL Toy: Poniżej przedstawiono przykład wypełnionego przez Sharon Jones Formularza odpowiedzialności w systemie:

Tabela 29. Formularz odpowiedzialności w systemie dla przedsiębiorstwa JKL Toy: przykład

Kto jest głównym szefem ochrony? Sharon Jones Kto jest szefem ochrony zajmującym się składowaniem?Ken Harrison			
Nazwa profilu	Nazwa użytkownika	Klasa	Uwagi
JONESS	Sharon Jones	*SECOFR	Sharon jest głównym szefem ochrony i menedżerem systemu.
HARRISOK	Ken Harrison	*SECOFR	Ken jest zastępcą Sharon jako ogólnego menedżera systemu.
JOHNSONS	Sandy Johnson	*SYSOPR	Sandy jest odpowiedzialna za działanie systemu oraz składowanie.
ROGERSK	Karen Rogers	*SYSOPR	Karen pomaga Sandy w operacjach oraz składowaniu systemu.
WILLISR	Rose Willis	*SYSOPR	Rose jest operatorem podczas drugiej zmiany.

Po wypełnieniu Formularza odpowiedzialności w systemie można rozpocząć wybieranie wartości dla każdego użytkownika.

Wybieranie wartości dla każdego użytkownika

Po określeniu odpowiedzialności użytkowników w systemie można rozpocząć wybieranie wartości dla każdego użytkownika. Planując profile grupowe jako wzorce dla pojedynczych profili użytkowników, wykonano większość pracy. Aby przypisać każdego użytkownika do prawidłowej grupy i zdefiniować sposób jego odróżniania od reszty użytkowników w grupie, należy użyć Formularza pojedynczego profilu użytkownika. Jeden Formularz pojedynczego profilu użytkownika należącego do danej grupy należy wypełnić jako przykład, a następnie wrócić do tego miejsca i przygotować formularze dla dodatkowych grup użytkowników.

U góry Formularza pojedynczego profilu użytkownika należy wpisać nazwę profilu grupowego oraz pozostałe informacje opisowe.

Przykład: informacje opisowe Formularza pojedynczego profilu użytkownika dla przedsiębiorstwa JKL Toy

Poniżej przedstawiono sposób wypełnienia górnej części Formularza pojedynczego profilu użytkownika przez Sharon Jones.

Tabela 30. Formularz pojedynczego profilu użytkownika dla przedsiębiorstwa JKL Toy: przykład informacji opisowych

Formularz pojedynczego profilu użytkownika	
Przygotowany przez: Sharon Jones	Data: 9/5/99
Nazwa profilu grupowego: WYDOP	
Właściciel tworzonych obiektów:	Uprawnienia grupy do tworzonych obiektów:

Tabela 30. Formularz pojedynczego profilu użytkownika dla przedsiębiorstwa JKL Toy: przykład informacji opisowych (kontynuacja)

Rodzaj uprawnień grupy:

Określanie wartości dla członków grupy

Na Formularzu pojedynczego profilu użytkownika należy napisać nazwę profilu oraz opis (nazwę użytkownika) każdego członka grupy. W poniższych paragrafach opisano, jak określić pozostałe wartości dla każdego członka grupy.

Należy pamiętać, że profil grupowy jest wzorcem dla pojedynczych profili użytkownika. Na Formularzu pojedynczego profilu użytkownika należy podać tylko te elementy, które są inne niż te w grupie.

- **Przypisywanie haseł**: najprostszym sposobem przypisywania haseł początkowych jest podanie haseł takich samych, jak nazwy profili. Następnie, po ustawieniu utraty ważności hasła, można zażądać, aby zostały one zmienione podczas pierwszego wpisania się. Temat Ustawianie utraty ważności hasła zawiera informacje, jak to zrobić automatycznie, podczas kopiowania profilu grupowego. W takim przypadku na Formularzu pojedynczego profilu użytkownika nie trzeba podawać listy haseł.
- **Klasa użytkownika i ograniczenie możliwości**: na Formularzu odpowiedzialności w systemie można sprawdzić, którzy członkowie grupy wymagają innych wartości dla pól **Klasa użytkownika** i **Ograniczenie możliwości**. Na Formularzu pojedynczego profilu użytkownika należy podać odpowiednie informacje dla każdego, kto wymaga wartości innych niż te z profilu grupowego.
- **Określanie pozostałych wartości**: należy sprawdzić, czy dany użytkownik wymaga wartości, które są inne niż te określone w Formularzu opisywania grupy. Na Formularzu opisywania grupy, pola **Klasa użytkownika** i **Ograniczenie możliwości** umieszczone są na górze, ponieważ ich wartości często różnią się dla niektórych członków grupy. Należy podać pozostałe pola, które zmieniają się w zależności od członka grupy, z którą użytkownik aktualnie pracuje.

Aby zakończyć tę czynność planowania, należy upewnić się, że:

- wypełniono Formularz wybierania wartości systemowych,
- w Formularzu konwencji nazewnictwa opisano, jakie nazewnictwo ma być zastosowane dla profili użytkowników,
- dla każdej grupy użytkowników w przedsiębiorstwie przygotowano Formularz pojedynczego profilu użytkownika.

Przed zaplanowaniem ochrony zasobów, warto zapoznać się z przykładem informacji użytych przez Sharon dla pojedynczych użytkowników.

Przykład: Formularz pojedynczego profilu użytkownika dla przedsiębiorstwa JKL Toy: W przedsiębiorstwie JKL Toy, osoby które pracują na rampie załadowczej, mogą uruchamiać tylko jeden program. Sharon ograniczyła tych użytkowników do kilku funkcji, ponieważ pracują w miejscu, w którym osoby postronne łatwo mogą uzyskać dostęp do stacji roboczych. Pracownicy magazynu mają program początkowy, ale nie mają menu początkowego. W dziale obsługi zamówień znajdują się dwie drukarki lokalne, a w zdalnym biurze sprzedaży jedna. Dlatego Sharon niektórych użytkowników przypisała do innej drukarki niż grupę.

Poniżej przedstawiono Formularz pojedynczego profilu użytkownika, który Sharon Jones wypełniła dla magazynu i działu obsługi zamówień w przedsiębiorstwie JKL Toy. Należy zauważyć, że wypełnione zostały tylko te pola, które są inne niż wartości w profilu grupowym.

Tabela 31. Formularz pojedynczego profilu użytkownika dla przedsiębiorstwa JKL Toy: przykład magazynu

Nazwy profilu grupowego: WYDWH					
Wpisy dotyczące każdego członka grupy:					
Profil użytkownika	**Tekst (opis)**	**Klasa użytkownika**	**Ograniczenie możliwości**	**Program początkowy/ Biblioteka**	**Menu początkowe/ Biblioteka**
WILLISR	Willis, Rose	*SYSOPR	*NO		

Tabela 31. Formularz pojedynczego profilu użytkownika dla przedsiębiorstwa JKL Toy: przykład magazynu (kontynuacja)

WAGNERR	Wagner, Ray			ICRCPT/ICPGMLIB	brak
AMESJ	Ames, Janice			ICRCPT/ICPGMLIB	brak
FOSSJ	Foss, Julie				
WOODBURC	Woodburt, Carol				

Tabela 32. Formularz pojedynczego profilu użytkownika: przykład działu obsługi zamówień

Nazwa profilu grupowego: WYDOP				
Wpisy dotyczące każdego członka grupy:				
Profil użytkownika	**Tekst (opis)**	**Klasa użytkownika**	**Ograniczenie możliwości**	**Drukarka**
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05
RICHARDK	Richards, Karen			
UNGERJ	Unger, Jeff			PRT04
BELLB	Bell, Brad			PRT04

Teraz można rozpocząć planowanie ochrony zasobów.

Planowanie ochrony zasobów

Po zakończeniu procesu planowania użytkowników systemu można zaplanować ochronę zasobów, która zabezpieczy obiekty w systemie. W sekcji ″Konfigurowanie ochrony zasobów″ znajdują się informacje na temat konfigurowania ochrony zasobów w systemie.

Wartości systemowe oraz profile użytkowników kontrolują dostęp do systemu oraz zapobiegają przed nieautoryzowanym wpisywaniem się użytkowników. Ochrona zasobów steruje działaniami podejmowanymi przez autoryzowanych użytkowników systemu po ich pomyślnym wpisaniu się. Ochrona zasobów obsługuje główne cele ochrony w systemie:

- poufność informacji,
- dokładność informacji, służąca zapobieganiu nieautoryzowanym zmianom,
- dostępność informacji, służąca zapobieganiu przypadkowym lub umyślnym uszkodzeniem.

W zależności od tego, czy przedsiębiorstwo samo tworzy aplikacje, czy je kupuje, można różnie zaplanować ochronę zasobów. Jeśli aplikacje powstają w przedsiębiorstwie, wymagania dotyczące ochrony informacji należy przekazać programiście już podczas procesu projektowania aplikacji. W przypadku zakupu aplikacji należy określić potrzeby ochrony i porównać je ze sposobem, w jaki dostawca zaprojektował aplikację. Opisane tutaj techniki powinny pomóc w obu przypadkach.

Ten temat udostępnia podstawowe podejście do planowania ochrony zasobów. Przedstawia główne techniki oraz prezentuje sposób ich wykorzystania. Opisane tutaj metody niekoniecznie muszą działać w przypadku każdego przedsiębiorstwa oraz każdej aplikacji. Podczas planowania ochrony zasobów należy skonsultować się z programistą lub dostawcą aplikacji.

W celu uzyskania pomocy podczas planowania ochrony zasobów, należy przejrzeć poniższe tematy:

- Określanie celów ochrony zasobów
- Typy uprawnień
- Planowanie ochrony bibliotek aplikacji
- Określanie praw własności dla bibliotek i obiektów

- Grupowanie obiektów
- Zabezpieczanie zbiorów wydruków
- Zabezpieczanie stacji roboczych
- Podsumowanie zaleceń dotyczących ochrony zasobów
- Planowanie instalowania aplikacji

Które formularze są potrzebne?

Należy wykonać kopie poniższych formularzy oraz wypełnić je w trakcie czytania tego tematu. Należy przejść przez cały proces dla jednej aplikacji i powtórzyć go dla wszystkich następnych.

Tabela 33. Formularze planowania potrzebne do zaplanowania ochrony zasobów

Nazwa formularza	Potrzebna liczba kopii
Formularz list autoryzacji	Kilka
Formularz ochrony zbiorów wydruków oraz stacji roboczej	Jeden

Do następujących formularzy, z którymi wcześniej pracowano, należy dodać informacje:

Tabela 34. Formularze planowania, które będą zmienione

Nazwa formularza	Przygotowany w
Formularz opisywania biblioteki	Opisywanie informacji dotyczących bibliotek
Formularz opisywania grupy użytkowników	Planowanie profili grupowych

Należy odnieść się do formularzy, które zostały wcześniej przygotowane:

Tabela 35. Formularze planowania potrzebne do zakończenia planowania ochrony zasobów

Nazwa formularza	Przygotowany w:
Formularz opisywania biblioteki	Rysowanie diagramu aplikacji i Identyfikowanie grup użytkowników
Formularz opisywania aplikacji	Opisywanie informacji aplikacji
Formularz pojedynczego profilu użytkownika	Wybieranie wartości dla każdego użytkownika
Formularz identyfikowania grupy użytkowników	Identyfikowanie grup użytkowników
Formularz odpowiedzialności w systemie	Określanie, kto powinien być odpowiedzialny za funkcje systemu
Formularz planowania ochrony fizycznej	Planowanie ochrony fizycznej

Określanie celów ochrony zasobów

Aby rozpocząć planowanie ochrony zasobów, najpierw należy zrozumieć jej cele. System iSeries udostępnia elastyczną implementację ochrony zasobów. Umożliwia ona zabezpieczenie krytycznych zasobów, w wymagany sposób. Ale ochrona zasobów przekłada się także na dodatkowy nakład pracy dla aplikacji. Na przykład gdy aplikacja potrzebuje obiektu, system musi sprawdzić uprawnienia użytkownika do tego obiektu. Należy zrównoważyć wymagania poufności oraz kosztów związanych z obniżeniem wydajności. Po dokonaniu wyboru ochrony zasobów, należy porównać wartość ochrony z jej kosztami.

Aby zapobiec obniżeniu wydajności aplikacji przez ochronę zasobów, należy zastosować się do następujących wskazówek.

- schemat ochrony zasobów powinien być prosty,
- należy zabezpieczać tylko te obiekty, które powinny być zabezpieczone,

- ochronę zasobów należy wykorzystywać jako uzupełnienie, a nie zastępstwo innych narzędzi służących do zabezpieczania informacji:
  - ograniczanie dostępu użytkowników do określonych menu oraz aplikacji,
  - zapobieganie wprowadzeniu przez użytkowników niektórych komend (ograniczanie możliwości w profilach użytkowników).

Planowanie ochrony zasobów należy rozpocząć od zdefiniowania własnych celów. Cele ochrony można zdefiniować w Formularzu opisywania aplikacji lub Formularzu opisywania biblioteki.

Używany formularz zależy od sposobu zorganizowania informacji w bibliotekach.

Przed przeglądnięciem rodzajów uprawnień, które mogą być wykorzystane do ochrony zasobów, można zapoznać się z przykładem celów ochrony przedsiębiorstwa JKL Toy.

Przykład: cele ochrony w przedsiębiorstwie JKL Toy

Sharon Jones z przedsiębiorstwa JKL Toy do opisywania wymagań ochrony dla biblioteki klientów (CUSTLIB) korzysta z Formularza opisywania biblioteki:

Tabela 36. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład celów ochrony

Formularz opisywania biblioteki	Część 1 z 2
Zdefiniowane cele ochrony biblioteki, określające czy zawiera poufne informacje:	Obecnie każdy w przedsiębiorstwie ma możliwość przeglądania informacji o klientach oraz ich zamówieniach. Aby zapewnić integralność informacji, należy nalezy dokładnie ustalić, kto może zmieniać te informacje.

Sharon użyła Formularza opisywania aplikacji dla aplikacji Kontrakty i wycena, aby opisać cele ochrony dla całej aplikacji.

Tabela 37. Formularz opisywania aplikacji dla przedsiębiorstwa JKL Toy: przykład celów ochrony

Formularz opisywania aplikacji	Część 1 z 2
Zdefiniowane cele ochrony biblioteki, określające czy zawiera poufne informacje:	Informacje na temat kontraktów i wyceny specjalnej są poufne. Tylko kilka osób jest upoważnionych do ich przeglądania oraz zmieniania: • personel działu sprzedaży i marketingu oraz wszyscy menedżerowie mogą tworzyć, zmieniać i analizować kontrakty; używają zarówno zbiorów jak i programów, • personel działu obsługi zamówień pośrednio zmienia kontrakty oraz przegląda ceny, gdy wprowadza i dostarcza zamówienia; osoby z tego działu nie mogą przeglądać kontraktów oraz cen, za wyjątkiem momentu wprowadzania lub zmieniania zamówienia.

Cele ochrony dla aplikacji należy zapisać w Formularzu opisywania aplikacji lub Formularzu opisywania biblioteki. Następnie można zapoznać się z typami uprawnień, które można wykorzystać do zaplanowania ochrony zasobów.

Typy uprawnień

Po określeniu celów ochrony zasobów oraz zapisaniu swoich decyzji w Formularzu opisywania biblioteki, można rozpocząć planowanie rodzajów uprawnień. Ochrona zasobów definiuje, jaki dostęp do obiektów w systemie mają użytkownicy.

Uprawnienie określa, w jaki sposób ktoś może korzystać z obiektu. Na przykład użytkownik może być uprawniony do przeglądania informacji lub do ich zmiany. System udostępnia kilka różnych rodzajów uprawnień. Firma IBM grupuje

te rodzaje uprawnień w kategorie, nazywane **uprawnieniami zdefiniowanymi w systemie**, które spełniają potrzeby większości użytkowników. Przedstawiona poniżej tabela zawiera kategorie uprawnień oraz opisuje, jak odnoszą się one do zabezpieczania plików i programów.

Uwaga: Podczas planowania uprawnień należy zapoznać się z poniższą tabelą.

Tabela 38. Uprawnienia zdefiniowane w systemie

Nazwa uprawnienia	Działania dozwolone w przypadku plików	Działania niedozwolone w przypadku plików	Działania dozwolone w przypadku programów	Działania niedozwolone w przypadku programów
*USE	Przeglądanie informacji z pliku.	Zmiana lub usuwanie informacji z pliku. Usuwanie pliku.	Uruchamianie programu.	Zmiana lub usuwanie programu.
*CHANGE	Przeglądanie, zmiana i usuwanie rekordów z pliku.	Usuwanie lub czyszczenie całego pliku.	Zmiana opisu programu.	Zmiana lub usuwanie programu.
*ALL	Tworzenie i usuwanie pliku. Dodawanie, zmiana i usuwanie rekordów z pliku. Autoryzowanie innych użytkowników do korzystania z pliku.	brak	Tworzenie, zmiana i usuwanie programu. Autoryzowanie innych użytkowników do korzystania z programu.	Zmiana właściciela programu, jeśli program adoptuje uprawnienia.
*EXCLUDE[1]	brak	Jakikolwiek dostęp do pliku.	brak	Jakikolwiek dostęp do programu.
1 Uprawnienie *EXCLUDE przesłania wszystkie uprawnienia, które są nadawane publicznie lub przez profil grupowy.				

Poznawanie sposobu współdziałania uprawnień do obiektu i do biblioteki

Aby zaprojektować prostą ochronę zasobów, należy spróbować zaplanować ochronę wszystkich bibliotek. Aby to zrobić, należy zrozumieć, w jaki sposób uprawnienia zdefiniowane w systemie stosowane są dla bibliotek. Prezentuje to poniższa tabela:

Tabela 39. Zdefiniowane w systemie uprawnienia do bibliotek

Nazwa uprawnienia	Działanie dozwolone	Działanie niedozwolone
*USE	• W przypadku obiektów w bibliotece, możliwe są działania dozwolone przez uprawnienie do określonego obiektu. • W przypadku biblioteki, przeglądanie informacji opisowych.	• Dodawanie nowych obiektów do biblioteki. • Zmiana opisu biblioteki. • Usuwanie biblioteki.
*CHANGE	• W przypadku obiektów w bibliotece, możliwe są działania dozwolone przez uprawnienie do określonego obiektu. • Dodawanie nowych obiektów do biblioteki. • Zmiana opisu biblioteki.	• Usuwanie biblioteki.
*ALL	• Dozwolone jest wszystko. • Usuwanie biblioteki. • Autoryzowanie innych użytkowników do korzystania z biblioteki.	• brak

Należy także zrozumieć, w jaki sposób współdziałają ze sobą uprawnienia do biblioteki i obiektu. Przedstawiona poniżej tabela prezentuje przykłady uprawnień wymaganych zarówno dla obiektu, jak i biblioteki:

Tabela 40. Teraz uprawnienia do biblioteki i obiektu współdziałają ze sobą

Rodzaj obiektu	Działania	Wymagane uprawnienia dla obiektu	Wymagane uprawnienia do biblioteki
Plik	Zmiana danych	*CHANGE	*USE
Plik	Usuwanie pliku	*ALL	*USE
Plik	Tworzenie pliku	*ALL	*CHANGE
Program	Uruchamianie programu	*USE	*USE
Program	Zmiana (ponowne kompilowanie) programu	*ALL	*CHANGE
Program	Usuwanie programu	*ALL	*USE

Uprawnienia do katalogu są podobne do uprawnień do biblioteki. Aby uzyskać dostęp do obiektu, należy mieć uprawnienia do wszystkich katalogów w nazwie ścieżki do tego obiektu.

Teraz można zaplanować ochronę bibliotek aplikacji.

Planowanie ochrony bibliotek aplikacji

Po określeniu celów ochrony zasobów można rozpocząć planowanie ochrony bibliotek aplikacji. Przed rozpoczęciem opisanego poniżej procesu należy wybrać jedną z bibliotek aplikacji. Jeśli pliki i programy przechowywane są w oddzielnych bibliotekach, należy wybrać bibliotekę, która zawiera pliki. Po zakończeniu tego tematu, należy powtórzyć wszystkie kroki dla pozostałych bibliotek aplikacji.

Należy przejrzeć zebrane informacje, które dotyczą aplikacji i bibliotek:

- formularz opisywania aplikacji,
- formularz opisywania biblioteki,
- formularz opisywania grupy dla wszystkich grup wymagających biblioteki,
- diagram aplikacji, bibliotek i grup użytkowników.

Należy zastanowić się, które grupy potrzebują informacji z tej biblioteki, dlaczego ich potrzebują oraz co potrzebują z nimi robić.

Określanie zawartości biblioteki

Biblioteki aplikacji zawierają ważne pliki aplikacji. Mogą także zawierać inne obiekty, z których większość to narzędzia programistyczne zapewniające poprawną pracę aplikacji. Są to:

- zbiory robocze,
- obszary danych i kolejki komunikatów,
- programy,
- zbiory komunikatów,
- komendy,
- kolejki wyjściowe.

Większość obiektów innych niż pliki i kolejki wyjściowe nie jest narażone na ryzyko naruszenia ochrony. Zazwyczaj zawierają małą ilość danych aplikacji, często w formacie, który nie jest zrozumiały poza programami. Za pomocą komendy Wyświetlenie biblioteki (Display Library) można wyświetlić listę nazw i opisów wszystkich obiektów w bibliotece. Na przykład aby wyświetlić listę zawartości biblioteki KONTRAKTY, należy wpisać: DSPLIB LIB(KONTRAKTY) OUTPUT(*PRINT)

Następnie należy zadecydować, jakie uprawnienia publiczne mają dotyczyć bibliotek aplikacji oraz bibliotek programów.

Decydowanie o uprawnieniach publicznych do bibliotek aplikacji

W zagadnieniach ochrony zasobów **publiczny** oznacza, każdą osobę autoryzowaną do wpisywania się do systemu. **Uprawnienia publiczne** umożliwiają użytkownikom dostęp do obiektu, chyba że określono bardziej specyficzny dostęp. Oprócz decydowania o uprawnieniach publicznych dla obiektów już znajdujących się w bibliotece, można określić uprawnienia do nowych obiektów, dodawanych później do biblioteki. Aby to zrobić można skorzystać z parametru **Tworzenie uprawnienia (Create Authority - CRTAUT)**. Zazwyczaj uprawnienia publiczne do obiektów biblioteki i uprawnienia do tworzenia nowych obiektów w bibliotece powinny być takie same.

Wartość systemowa QCRTAUT (Tworzenie uprawnienia - Create Authority) określa uprawnienia publiczne do nowych obiektów w całym systemie. Firma IBM dostarcza wartość systemową QCRTAUT z ustawieniem *CHANGE. Należy unikać zmieniania wartości QCRTAUT, ponieważ korzysta z niej wiele funkcji. Jeśli dla parametru Tworzenie uprawnienia (Create Authority - CRTAUT) biblioteki aplikacji podana zostanie wartość *SYSVAL, wykorzystywana jest wartość systemowa QCRTAUT (*CHANGE).

Aby wszystko uprościć i zwiększyć wydajność, uprawnień publicznych należy używać wszędzie, gdzie jest to możliwe. Aby określić, jakie uprawnienia publiczne powinna mieć biblioteka, należy zadać następujące pytania:

- Czy każda osoba w przedsiębiorstwie ma dostęp do większości informacji w tej bibliotece?
- Jaki rodzaj dostępu do większości informacji w tej bibliotece powinni mieć pracownicy?

Należy skoncentrować się na decyzjach dotyczących większości osób oraz większości informacji. Następnie należy zapoznać się z informacjami o tym, jak radzić sobie z wyjątkami. Planowanie ochrony zasobów często jest powtarzającym się procesem. Po rozważeniu wymagań dla określonego obiektu może się okazać, że należy wprowadzić zmiany w uprawnieniach publicznych. Przed wybraniem jednego rodzaju uprawnień, które będą spełniać wymagania ochrony oraz wydajności, należy wypróbować kombinacje uprawnień publicznych i prywatnych dla obiektu oraz biblioteki.

Upewnianie się, czy uprawnienia są wystarczające

Uprawnienia *CHANGE dla obiektów oraz *USE do biblioteki są wystarczające dla większości funkcji aplikacji. Jednak aby określić, czy pewne funkcje aplikacji wymagają większych uprawnień, należy zadać kilka pytań programiście lub dostawcy aplikacji:

- Czy podczas przetwarzania z biblioteki usuwane są jakiekolwiek zbiory lub inne obiekty? Czy usuwana jest zawartość zbiorów? Czy do zbiorów są dodawane podzbiory? Usuwanie obiektu, czyszczenie zbioru lub dodawanie podzbiorów wymaga uprawnień *ALL dla obiektu.
- Czy podczas przetwarzania w bibliotece tworzone są jakiekolwiek pliki, zbiory lub inne obiekty? Tworzenie obiektu wymaga uprawnienia *CHANGE do biblioteki.

Przed zadecydowaniem o uprawnieniach specjalnych do bibliotek programów warto zapoznać się z przykładem wyborów dokonanych przez Sharon dotyczących uprawnień do obiektów.

Przykład: Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy:

Sharon Jones przejrzała cele ochrony dla biblioteki klientów, a także informacje na temat aplikacji oraz działów, które korzystają z informacji o klientach. Zrobiła notatki na temat swoich wniosków:

- Każdy dział, poza magazynem i produkcją, wprowadza zmiany w informacjach o klientach.
- Wszyscy użytkownicy z magazynu i produkcji mają profile użytkowników z Ograniczeniem możliwości (wartość Tak) i mają dostęp tylko do niektórych menu i programów. Ich menu umożliwiają przeglądanie informacji o klientach, ale nie pozwalają na ich zmienianie.

- Uprawnienia publiczne dla obiektów w bibliotece klientów powinny być ustawione na wartość *CHANGE. Ograniczenia menu zabezpieczają przed wprowadzaniem zmian w informacjach o klientach przez osoby niepowołane. Jednak należy ocenić, czy w późniejszym czasie do systemu będą dodawane pozostałe działy.

To jest przykład łagodnego podejścia do ochrony informacji. W takim przypadku wyjątki obsługiwane są przez profile użytkowników, a nie przez używanie ograniczeń w uprawnieniach. Dla biblioteki klientów (CUSTLIB) Sharon wypełniła część Formularza opisywania biblioteki dotyczącą uprawnień publicznych.

Tabela 41. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy — część 1: przykład biblioteki klientów

Nazwa biblioteki: CUSTLIB	Nazwa opisowa (tekst): Biblioteka klientów
Uprawnienia publiczne do biblioteki:	*USE
Uprawnienia publiczne dla obiektów w bibliotece:	*CHANGE
Uprawnienia publiczne dla nowych obiektów (CRTAUT):	*CHANGE

Sharon Jones odkryła, że zawartość niektórych plików tymczasowych z biblioteki klientów jest usuwana podczas przetwarzania na koniec miesiąca przez aplikację Należności. Zadecydowała, że uprawnienia do tych plików nada pojedynczo i nie będzie podejmowała ryzyka, że te obiekty mogą zostać usunięte przypadkowo. Dla pozostałych działań związanych z przetwarzaniem, wystarczające są uprawnienia *CHANGE.

Ponieważ tylko kilka osób uruchamia proces przetwarzania na koniec miesiąca, Sharon nie uważa, że pliki tymczasowe są wystawione na ryzyko związane z ochroną. Zadecydowała, że nada uprawnienia publiczne *ALL do tych plików zamiast zmieniać uprawnienia tylko użytkownikom, którzy wykonują przetwarzanie na koniec miesiąca. Przedstawiona poniżej tabela zawiera drugą część Formularza opisywania biblioteki dla biblioteki klientów:

Tabela 42. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy — część 2: przykład biblioteki klientów

Lista uprawnień szczegółowych dla obiektów biblioteki				
Profil grupowy lub użytkownika	Nazwa obiektu	Rodzaj obiektu	Wymagane uprawnienia	Lista autoryzacji
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

Teraz można zadecydować o uprawnieniach publicznych do bibliotek zawierających programy.

Decydowanie o uprawnieniach publicznych do bibliotek programów

Często programy użytkowe przechowywane są w bibliotece innej niż pliki i inne obiekty. Nie jest konieczne korzystanie z oddzielnych bibliotek dla aplikacji, ale wielu programistów korzysta z tej techniki podczas projektowania aplikacji. Jeśli aplikacja ma oddzielne biblioteki programów, należy zdecydować o uprawnieniach publicznych do tych bibliotek. Uprawnienie *USE można wykorzystać zarówno dla biblioteki, jak i dla programów w bibliotece - w celu uruchamiania programów - ale w bibliotekach programów mogą być inne obiekty, które wymagają dodatkowych uprawnień. Programiście należy zadać następujące pytania:

- Czy aplikacja podczas komunikowania się z programami korzysta z obszarów danych lub kolejek komunikatów? Czy znajdują się one w bibliotece programów? Do obsługi obszarów danych oraz kolejek komunikatów wymagane jest uprawnienie *CHANGE do obiektu.
- Czy podczas przetwarzania z biblioteki programów usuwane są jakiekolwiek obiekty, na przykład obszary danych? Do usuwania obiektu wymagane jest uprawnienie *ALL do obiektu.
- Czy podczas przetwarzania w bibliotece programów tworzone są jakiekolwiek obiekty, na przykład obszary danych? Do tworzenia nowych obiektów w bibliotece wymagane jest uprawnienie *CHANGE do biblioteki.

W Formularzu opisywania biblioteki w obu częściach należy podać wszystkie informacje dotyczące ochrony zasobów, poza właścicielem biblioteki oraz kolumną listy autoryzacji. Następnie można określić prawo własności do bibliotek i obiektów.

Można zapoznać się z dwoma przykładami, jak Sharon Jones określiła uprawnienia do bibliotek programów. W pierwszym przykładzie Sharon zdecydowała, że dla biblioteki programu Zamówienia klientów wystarczające jest łagodne podejście. W drugim przykładzie przedstawiono bardziej ścisłe podejście, które Sharon zastosowała dla biblioteki programu Należności.

Przykład: Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy — podejście nierestrykcyjne: Sharon Jones zbadała bibliotekę programu Zamówienia klientów i zrobiła następujące notatki:

- Do komunikowania się między programami wykorzystywana jest jedna kolejka komunikatów - COMSGQ01.
- Zawartość kolejki jest usuwana, ale sama kolejka nigdy nie jest usuwana. Wystarczające dla kolejki są uprawnienia *CHANGE.

Zadecydowała się nadać uprawnienia *USE dla wszystkich obiektów w bibliotece programu oraz oddzielnie zdefiniować kolejkę komunikatów COMSGQ01. Przedstawione poniżej dwie tabele prezentują jej Formularz opisywania biblioteki dla biblioteki COPGMLIB:

Tabela 43. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład biblioteki programu

Formularz opisywania biblioteki	**Część 1 z 2**
Nazwa biblioteki: COPGMLIB	Nazwa opisowa (tekst): Biblioteka programu Zamówienia klientów
Uprawnienia publiczne do biblioteki: *USE Uprawnienia publiczne dla obiektów biblioteki: *USE Uprawnienia publiczne dla nowych obiektów (CRTAUT): *USE Właściciel biblioteki:	

Tabela 44. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład biblioteki programu

Formularz opisywania biblioteki				**Część 2 z 2**
Lista uprawnień dla pojedynczych obiektów w bibliotece				
Profil grupowy lub profil użytkownika	Nazwa obiektu	Rodzaj obiektu	Wymagane uprawnienia	Listy autoryzacji
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

Korzystanie z uprawnień do programu w celu kontrolowania dostępu

Mimo że większość osób w przedsiębiorstwie JKL Toy może zmieniać informacje o klientach, tylko kilka może ustalać dla nich limity kredytowe. Limity kredytowe są przechowywane w zbiorze głównym klientów (CUSTMAS), ale zmieniane są za pomocą oddzielnego programu ARPGM12 z biblioteki ARPGMLIB. Sharon może ograniczyć dostęp do tegoten programu, aby zapobiec zmienianiu limitów kredytowych przez osoby niepowołane. Przedstawione poniżej tabele prezentują Formularz opisywania biblioteki dla biblioteki ARPGMLIB:

Tabela 45. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład pojedynczych uprawnień

Formularz opisywania biblioteki	**Część 1 z 2**
Nazwa biblioteki: ARPGMLIB	Nazwa opisowa (tekst): Biblioteka programu Należności

Tabela 45. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład pojedynczych uprawnień (kontynuacja)

Uprawnienia publiczne do biblioteki: *USE
Uprawnienia publiczne dla obiektów biblioteki: *USE
Uprawnienia publiczne dla nowych obiektów (CRTAUT): *USE
Właściciel biblioteki:

Tabela 46. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład pojedynczych uprawnień

Formularz opisywania biblioteki				**Część 2 z 2**
Lista uprawnień dla pojedynczych obiektów w bibliotece				
Profil grupowy lub profil użytkownika	Nazwa obiektu	Rodzaj obiektu	Wymagane uprawnienia	Listy autoryzacji
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

Przed rozpoczęciem ustalania praw własności do bibliotek i obiektów, można zapoznać się z restrykcyjnym przykładem, który korzysta z uprawnień adoptowanych.

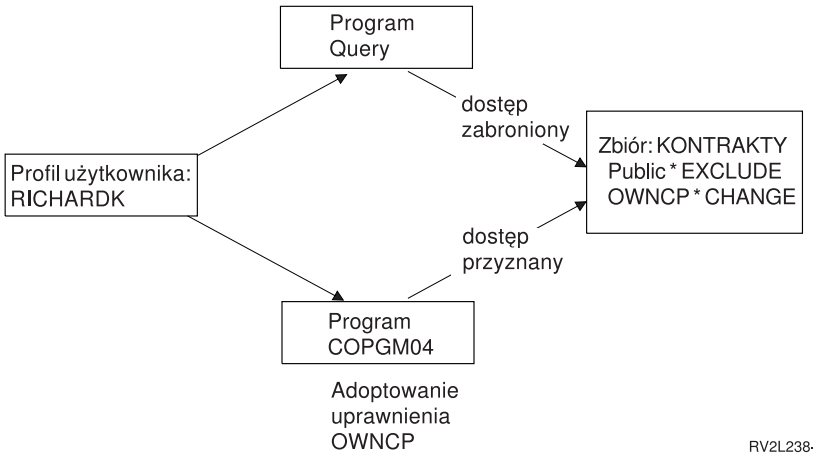
Przykład: Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy — podejście restrykcyjne: Przykłady przedstawione do tej pory prezentowały łagodne podejście do ochrony, gdy większość osób miała dostęp do informacji w bibliotece. Informacje na temat kontraktów i wyceny w przedsiębiorstwie JKL Toy uważane są za informacje poufne i wymagają podejścia restrykcyjnego. Na szczęście wszystkie te informacje przechowywane są w oddzielnej bibliotece. Programy do aktualizowania kontraktów i wycen także znajdują się w specjalnej bibliotece.

Sharon przejrzała cele ochrony dla aplikacji Kontrakty i wycena (sekcja Określanie celów dla ochrony zasobów). Przejrzała także Formularz opisywania aplikacji oraz Formularz opisywania biblioteki. Stwierdziła, że spełnienie celów ochrony dla aplikacji będzie trudne. Zrobiła kilka notatek i omówiła problem z dostawcą aplikacji:

- Pracownicy i menedżerowie z działu sprzedaży i marketingu tworzą i zmieniają kontrakty. Używają zarówno zbiorów, jak i programów.
- Pracownicy Obsługi zamówień zmieniają kontrakty i pośrednio przeglądają ceny podczas wprowadzania zamówień dostaw, ale nie mogą przeglądać kontraktów i cen w inny sposób. Jednak do tworzenia własnych raportów na temat klientów i zamówień będą używać programu Query. Jeśli będą mieli uprawnienia do plików aplikacji Kontrakty i wycena, będą mogli tworzyć programy Query służące do przeglądania lub drukowania.

Dostawca aplikacji dla przedsiębiorstwa JKL Toy, aby rozwiązać problem zasugerował użycie opcji uprawnień adoptowanych. **Uprawnienia adoptowane** umożliwiają użytkownikom adoptowanie uprawnień właściciela programu podczas jego uruchamiania. Użytkownik nie potrzebuje uprawnień do obiektu.

Przedstawiony poniżej diagram prezentuje przykład działania uprawnień adoptowanych. Karen Richards (RICHARDK) z działu obsługi klienta normalnie nie ma uprawnień do korzystania z pliku kontraktów. Jednak podczas wprowadzania zamówień musi sprawdzić i zaktualizować salda kontraktu. Program wprowadzania zamówień, który pracuje z saldami kontraktu (COPGM04), adoptuje uprawnienia profilu OWNCP. Gdy Karen uruchamia program COPGM04, ma uprawnienia do korzystania z pliku kontraktów:



Szczegółowe informacje na temat praw własności dla obiektu, zawiera temat ″Określanie praw własności do bibliotek i obiektów″. Dostawca aplikacji lub programista mogą określić, że podczas tworzenia (kompilowania) program adoptuje uprawnienia właściciela. Za pomocą komendy Zmiana programu (Change Program - CHGPGM) programista może ustawić adoptowanie uprawnień przez program. Przed użyciem tej techniki należy się upewnić, że zrozumiano działanie wszystkich funkcji programu.

Sharon zadecydowała o użyciu funkcji adoptowania uprawnień, aby umożliwić dostęp do plików aplikacji Kontrakty i wycena osobom spoza działu sprzedaży i marketingu. Określiła także, że wystarczającym uprawnieniem dla wszystkich obiektów używanych przez aplikację Kontrakty i wycena jest uprawnienie *CHANGE. Przedstawiona poniżej tabela prezentuje Formularz opisywania biblioteki dla biblioteki kontraktów:

Tabela 47. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład uprawnień restrykcyjnych

Formularz opisywania biblioteki		**Część 1 z 2**
Nazwa biblioteki: KONTRAKTY	Nazwa opisowa (tekst): Biblioteka programu Kontrakty i wycena	
Uprawnienia publiczne do biblioteki: *EXCLUDE Uprawnienia publiczne dla obiektów biblioteki: *CHANGE Uprawnienia publiczne dla nowych obiektów (CRTAUT): *CHANGE Właściciel biblioteki:		

Tabela 48. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład uprawnień restrykcyjnych

Formularz opisywania biblioteki				**Część 2 z 2**
Lista uprawnień dla pojedynczych obiektów w bibliotece				
Profil grupowy lub profil użytkownika	Nazwa obiektu	Rodzaj obiektu	Wymagane uprawnienia	Listy autoryzacji
DPTSM	KONTRAKTY	*LIB	*USE	
DPTMG	KONTRAKTY	*LIB	*USE	

Nie trzeba ograniczać uprawnień dla obiektów w bibliotece, ponieważ ograniczono dostęp do samej biblioteki. Sharon nadała uprawnienia menedżerom oraz działowi sprzedaży i marketingu. Użyła uprawnień grupowych, zamiast nadawania uprawnień pojedynczym osobom w działach.

Uwaga: Dobrze poinformowany programista, który ma dostęp do biblioteki, mógłby uzyskać dostęp do obiektów w bibliotece, nawet po odebraniu uprawnień do niej. Jeśli biblioteka zawiera obiekty z wysokimi wymaganiami ochrony, należy zabezpieczyć zarówno obiekty, jak i bibliotekę.

Przed rozpoczęciem określania praw własności do bibliotek i obiektów można zapoznać się z nierestrykcyjnym przykładem, który korzysta z uprawnień publicznych.

Określanie praw własności do bibliotek i obiektów

Po zaplanowaniu ochrony bibliotek aplikacji można ustawić prawa własności do bibliotek i obiektów. Podczas tworzeniaobiektu jest do niego przypisywany właściciel. Właściciel obiektu automatycznie zyskuje wszystkie prawa do tego obiektu, które obejmują autoryzowanie innych użytkowników do korzystania z obiektu, zmienianie obiektu oraz usuwanie go. Szef ochrony może wykonywać te funkcje na wszystkich obiektach w systemie.

System podczas śledzenia uprawnień do obiektu korzysta z profilu właściciela. System wykonuje tę czynność wewnętrznie. Może to bezpośrednio nie wpływać na profil użytkownika. Jednak jeśli prawo własności dla obiektu nie zostanie poprawnie zaplanowane, profile użytkowników mogą znacznie się powiększyć.

Kiedy system składuje obiekt, składuje taże nazwę profilu właściciela. Te informacje używane są podczas odtwarzania obiektu. Jeśli profilu właściciela odtwarzanego obiektu nie ma w systemie, system przesyła prawo własności do profilu QDFTOWN, który dostarczany jest przez firmę IBM.

Zalecenia

Poniższe zalecenia mają zastosowanie do wielu sytuacji, jednak nie do wszystkich. Po zapoznaniu się z zaleceniami, pomysły dotyczące praw własności dla obiektów należy omówić z programistą lub dostawcą aplikacji. W przypadku kupowania aplikacji może się zdarzyć, że nie będzie można kontrolować, który profil będzie właścicielem bibliotek i obiektów. Aplikacja może zapobiegać zmianie prawa własności.

- Należy unikać stosowania profili QSECOFR lub QPGMR, które dostarczane są przez firmę IBM, jako właścicieli aplikacji. Te profile mają prawa własności do wielu obiektów w bibliotekach dostarczanych przez IBM i z tego powodu już są bardzo duże.
- Również profil grupowy nie powinien być właścicielem aplikacji. Każdy członek grupy ma takie same uprawnienia jak profil grupowy, chyba że przypisano mu mniejsze uprawnienia. W efekcie, każdy członek grupy będzie miał pełne uprawnienia do aplikacji.
- Jeśli planuje się przekazanie odpowiedzialności związanych z kontrolowaniem aplikacji na menedżerów w różnych działach, to powinni oni mieć prawa własności do wszystkich obiektów aplikacji. Jednak menedżer aplikacji może zmienić odpowiedzialność. W takim przypadku prawo własności dla obiektów aplikacji, można przenieść na nowego menedżera.
- Wiele osób korzysta z techniki tworzenia specjalnego profilu właściciela aplikacji z hasłem o wartości *NONE. Profil właściciela jest używany przez system do zarządzania uprawnieniami do aplikacji. Szef ochrony (lub ktoś z takimi uprawnieniami) przeprowadza bieżące zarządzanie aplikacją lub to zadanie przekazywane jest menedżerom z uprawnieniem *ALL do danej aplikacji.

Należy zadecydować, które profile powinny być właścicielami aplikacji. W każdym Formularzu opisywania biblioteki należy wpisać profil właściciela.

Przed rozpoczęciem decydowania o prawie własności oraz dostępie do bibliotek użytkowników można przejrzeć przykład pokazujący, w jaki sposób przedsiębiorstwo JKL Toy określiło prawo własności do aplikacji.

Przykład: prawa własności dla aplikacji dla przedsiębiorstwa JKL Toy

Sharon Jones zadecydowała o utworzeniu dla każdej aplikacji specjalnego profilu właściciela. Ona i Ken Harrison, szef ochrony kopii zapasowych, wezmą na siebie odpowiedzialność za zarządzanie ochroną aplikacji. Później, gdy wymagania ochrony przedsiębiorstwa staną się bardziej złożone, Sharon może delegować odpowiedzialność za zarządzanie uprawnieniami menedżerom działów.

Do Formularza konwencji nazewnictwa dodała nową pozycję:

Tabela 49. Formularz konwencji nazewnictwa dla przedsiębiorstwa JKL Toy: przykład profilu właściciela

Typ obiektu	Konwencja nazewnictwa
Profil właściciela	Profil właściciela będzie tworzony dla każdej aplikacji. Będzie właścicielem wszystkich bibliotek aplikacji oraz znajdujących się w nich obiektów. Profil właściciela będzie nazywany OWN plus nazwa skrócona aplikacji. Profil właściciela aplikacji Kontrola zapasów będzie miał nazwę OWNIC.

Sharon zadecydowała, aby nazwa każdego profilu właściciela rozpoczynała się od OWN, aby wszystkie profile właścicieli na ekranach i listach pojawiały się razem.

Sharon przypisała właścicieli do wszystkich bibliotek aplikacji i wpisała te informacje na Formularzach konwencji nazewnictwa. Jedyną biblioteką, która ma więcej niż jednego możliwego właściciela aplikacji jest biblioteka klientów. Ponieważ aplikacja Należności jest używana do tworzenia nowych klientów oraz ustalania limitów kredytowych, Sharon zadecydowała, że powinna być właścicielem zbiorów klientów. Oto właściciele, których przypisała:

Nazwa biblioteki	Nazwa właściciela
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
KONTRAKTY	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

Teraz można zadecydować o prawach własności i dostępie do bibliotek użytkowników.

Decydowanie o prawie własności i dostępie do bibliotek użytkowników

Jeśli w systemie zainstalowany jest program licencjonowany IBM Query for iSeries lub inny program wspomagający podejmowanie decyzji, użytkownicy potrzebują biblioteki do przechowywania tworzonych programów zapytań. Zazwyczaj jest to **bieżąca biblioteka** w profilu użytkownika. Więcej informacji na temat tworzenia bieżącej biblioteki dla każdego użytkownika zawiera sekcja ″Wybieranie wartości systemowych, które wpływają na wpisywanie się.″ Sharon Jones planuje wykorzystanie bieżących bibliotek w przypadku działu sprzedaży i marketingu oraz bibliotek grupowych dla innych działów:

- Osoby z działu sprzedaży i marketingu często będą korzystać z programu Query. Każdy użytkownik powinien mieć prywatną bibliotekę. W przeciwnym przypadku będą musieli martwić się o to, jak nazywać swoje zapytania, a także przypadkowo będą mogli usunąć programy innych użytkowników.
- Pozostałe działy będą miały biblioteki grupowe. Jeśli ich pracownicy będą tworzyli wiele zapytań Query, trzeba będzie rozważyć wykorzystanie indywidualnych bibliotek.

Jeśli użytkownik należy do grupy, pole w profilu użytkownika służy do określania, czy użytkownik lub grupa ma prawa własności dla obiektów tworzonych przez użytkownika. Jeśli użytkownik jest właścicielem obiektu, można określić, jakie uprawnienia do tego obiektu będą mieli inni członkowie grupy. Można także określić, czy uprawnienia grupy są podstawowymi uprawnieniami grupy, czy prywatnymi. Podstawowe uprawnienia grupy mogą zwiększyć wydajność systemu. Sharon zrobiła kilka dodatkowych notatek dotyczących bibliotek użytkowników:

- osoby, a nie grupa z działu sprzedaży i marketingu powinny mieć prawa własności do tworzonych przez siebie obiektów; nie muszą zmieniać programów zapytań innych osób,
- każdy członek grupy powinien być w stanie uruchamiać zapytania innych użytkowników, co oznacza, że grupa ma uprawnienia *USE do wszystkich obiektów tworzonych przez członków grupy,
- uprawnienia grupy powinny być podstawowymi uprawnieniami grupy,
- użytkownicy publiczni nie mogą mieć dostępu do tych bibliotek; pracownicy działu sprzedaży i marketingu mogą generować pliki wyjściowe ze swoich zapytań; te pliki mogą zawierać poufne dane,

- w przypadku pozostałych działów, grupa będzie miała prawo własności do biblioteki grupy oraz wszystkich obiektów tworzonych w bibliotece; oznacza to, że każdy członek grupy może zmienić lub usunąć wszystko z biblioteki; jeśli będzie to powodowało problemy, spróbujemy innej metody.

Przedstawiona poniżej tabela prezentuje Formularz pojedynczego profilu użytkownika dla działu sprzedaży i marketingu, który korzysta z obiektów, do których prawa mają użytkownicy:

Tabela 50. Formularz pojedynczego profilu użytkownika przedsiębiorstwa JKL Toy: właścicielami obiektów są użytkownicy

Nazwa profilu grupowego: DPTSM	
Właściciel tworzonych obiektów: *USRPRF	Uprawnienia grupy do tworzonych obiektów: *USE
Rodzaj uprawnień grupy: *PGP	

Przedstawiona poniżej tabela prezentuje Formularz pojedynczego profilu użytkownika dla działu, w którym właścicielem obiektów jest grupa:

Tabela 51. Formularz pojedynczego profilu użytkownika przedsiębiorstwa JKL Toy: właścicielem obiektówjest grupa

Nazwa profilu grupowego: DPTxx	
Właściciel tworzonych obiektów: *GRPPRF	Uprawnienia grupy do tworzonych obiektów:

Jeśli właścicielem tworzonych obiektów jest grupa, pole **Uprawnienia grupy do tworzonych obiektów** nie jest wykorzystywane. Członkowie grupyautomatycznie otrzymują uprawnienie *ALL do wszystkich tworzonych obiektów.

Należy zadecydować, kto powinien być właścicielem i mieć dostęp do bibliotek użytkowników. W Formularzu pojedynczego profilu użytkownika w polach **Właściciel tworzonych obiektów** i **Uprawnienia grupy do obiektów** należy wpisać dokonane wybory. Teraz można rozpocząć grupowanie obiektów.

Grupowanie obiektów

Po określeniu prawa własności do bibliotek i obiektów, można rozpocząć grupowanie obiektów systemu. Aby uprościć zarządzanie uprawnieniami, należy skorzystać z list autoryzacji, aby pogrupować obiekty o takich samych wymaganiach. Następnie, zamiast nadawać uprawnienia do pojedynczych obiektów na liście, można nadać uprawnienia publiczne, profili grupowych i profili użytkowników do listy autoryzacji. System tak samo traktuje wszystkie obiekty, które są chronione przez listę autoryzacji, ale różnym użytkownikom można nadawać różne uprawnienia do całej listy.

Lista autoryzacji ułatwia ponowne ustanawianie uprawnień po odtwarzaniu obiektów. Jeśli obiekty są chronione przez listę autoryzacji, proces odtwarzania automatycznie dowiązuje obiekty do listy.

Grupie lub użytkownikowi można nadać uprawnienia do zarządzania listą autoryzacji (*AUTLMGT). Zarządzanie listą autoryzacji umożliwia użytkownikowi dodawanie i usuwanie z listy innych użytkowników oraz zmianę uprawnień dla tych użytkowników.

Zalecenia

- List autoryzacji należy używać dla obiektów, które wymagają zabezpieczeń i które mają podobne wymagania ochrony. Używanie list autoryzacji zachęca do myślenia o kategoriach uprawnień a nie o pojedynczych uprawnieniach. Listy autoryzacji ułatwiają także odtwarzanie obiektów oraz kontrolowanie uprawnień w systemie.
- Należy unikać skomplikowanych schematów, które łączą listy autoryzacji, uprawnienia grupowe oraz uprawnienia pojedyncze. Należy wybrać metodę najlepiej odpowiadającą wymaganiom, a nie używać wszystkich metod.

Konwencje nazewnictwa dotyczące list autoryzacji także należy dodać do Formularza konwencji nazewnictwa.

Po przygotowaniu Formularza listy autoryzacji, należy wrócić i dodać informacje do Formularza opisywania biblioteki. Programista lub dostawca aplikacji mógł wcześniej utworzyć listy autoryzacji. Należy to sprawdzić.

Przed zaplanowaniem ochrony drukarek i wydruków przydatne może być zapoznanie się z przykładem planowania list autoryzacji w przedsiębiorstwie JKL Toy przez Sharon Jones.

Przykład: Formularz list autoryzacji dla przedsiębiorstwa JKL Toy

Sharon przejrzała Formularz opisywania biblioteki dla biblioteki klientów i zadecydowała o utworzeniu listy autoryzacji dla zbiorów, których zawartość jest usuwana na koniec miesiąca. Chociaż są tylko trzy takie zbiory, to użycie listy autoryzacji ułatwi zarządzanie uprawnieniami. Jeśli do procesu na koniec miesiąca później zostaną dodane inne pliki, będzie je mogła łatwo zabezpieczyć za pomocą listy autoryzacji. Aby zabezpieczyć się przed niezamierzonymi problemami związanymi z przetwarzaniem na koniec miesiąca, Sharon zadecydowała o wykluczeniu dostępu publicznego do tych plików. Uprawnienia *ALL nadała tylko tym użytkownikom, którzy wykonują przetwarzanie. Rose Willis, operator systemu na drugiej zmianie, może potrzebować przeglądać informacje o zbiorach, aby sprawdzać przetwarzanie na koniec miesiąca. Wymaga uprawnień *USE.

Przedstawiona poniżej tabela prezentuje konwencje nazewnictwa, których Sharon użyła dla list autoryzacji.

Tabela 52. Formularz konwencji nazewnictwa dla przedsiębiorstwa JKL Toy: przykład listy autoryzacji

Formularz konwencji nazewnictwa	
Przygotowany przez: Sharon Jones	Data: 9/5/99
Typ obiektu	**Konwencja nazewnictwa**
Listy autoryzacji	Dla list zabezpieczających obiekty z jednej biblioteki, należy użyć nazwy biblioteki oraz liter LST i liczby. Lista dla obiektów w bibliotece CUSTLIB będzie miała nazwę CUSTLST1. Dla listy zabezpieczającej obiekty z więcej niż jednej biblioteki, jeśli to możliwe należy użyć nazwy skróconej aplikacji: ARLST1. Jeśli lista odnosi się do wielu aplikacji, należy wybrać znaczącą nazwę. Opis listy powinien odzwierciedlać jej główne przeznaczenie.

Zaprezentowana poniżej tabela przedstawia Formularz list autoryzacji dla biblioteki CUSTLIB. Sharon przygotowała ten formularz korzystając z informacji z Formularza opisywania biblioteki:

Tabela 53. Plan listy autoryzacji dla przedsiębiorstwa JKL Toy: przykład

Formularz list autoryzacji					
Nazwa listy autoryzacji: CUSTLST1					
Opis: Pliki, których zawartość usuwana jest podczas przetwarzania na koniec miesiąca.					
Obiekty chronione przezlistę					
Nazwa obiektu	Rodzaj obiektu	Biblioteka obiektu	Nazwa obiektu	Rodzaj obiektu	Biblioteka obiektu
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
Lista grup i użytkowników, którzy mają dostęp do listy					
Grupa lub użytkownik	Dozwolony rodzaj dostępu	Zarządzanie listą?	Grupa lub użytkownik	Dozwolony rodzaj dostępu	Zarządzanie listą?
PUBLIC	*EXCLUDE	nie	ROSSG	*ALL	nie
SMITHJ	*ALL	nie	JONESS	*ALL	tak
WILLISR	*USE	nie			

Do Formularza opisywania biblioteki Sharon dodała także informacje o liście autoryzacji dla biblioteki CUSTLIB:

Formularz opisywania biblioteki	Część 2 z 2

Przygotowany przez: Sharon Jones			Data: 9/9/99	
Nazwa biblioteki: CUSTLIB				
Lista uprawnień szczegółowych dla obiektów biblioteki				
Profil grupowy lub profil użytkownika	Nazwa obiektu	Rodzaj obiektu	Wymagane uprawnienia	Lista autoryzacji
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

Należy zauważyć, że aby używać listy autoryzacji, która określa uprawnienia publiczne, to uprawnienia publiczne dla każdego pliku muszą być zmienione na *AUTL.

W Formularzach opisywania biblioteki należy sprawdzić uprawnienia grupowe i pojedyncze. Należy zadecydować, czy używanie list autoryzacji jest odpowiednie. Jeśli tak, to należy przygotować Formularze list autoryzacji i zaktualizować informacjami o tych listach Formularze opisywania biblioteki. Następnie można zaplanować ochronę drukarek i zbiorów wydruków.

Planowanie ochrony drukarek oraz zbiorów wydruków

Po zgrupowaniu obiektów należy zaplanować sposób zabezpieczenia zbiorów wydruków. Wcześniej opracowano plany zabezpieczania informacji przechowywanych w systemie. Należy także zaplanować zabezpieczanie poufnych informacji podczas ich drukowania lub gdy oczekują na wydrukowanie. Należy sprawdzić Plan ochrony fizycznej dotyczący drukarek, z którego przedsiębiorstwo korzysta dla poufnych wydruków.

Jeśli używany jest program drukujący raporty, taki raport zazwyczaj nie jest bezpośrednio wysyłany do drukarki. Program tworzy kopię raportu, który nazywany jest **zbiorem buforowym** lub **zbiorem wydruku**. Do czasu udostępnienia drukarki zbiór buforowy przechowywany jest przez system w obiekcie zwanym **kolejką wyjściową**. Jeśli kolejka wyjściowa zawiera zbiór wydruku, można przeglądać go na swojej stacji roboczej. Można go także wstrzymać lub skierować do określonej drukarki.

Buforowanie ułatwia planowanie zadań drukowania oraz współużytkowanie drukarek. Ułatwia także zabezpieczanie wydruków poufnych. Do przechowywania oraz ograniczania możliwości przeglądania wydruków poufnych można tworzyć więcej specjalnych kolejek wyjściowych, a następnie zarządzać nimi. Można także kontrolować, kiedy wydruk poufny jest wysyłany z kolejki do drukarki.

Podczas pracy z tym tematem należy wypełniać Formularz ochrony zbiorów wydruków oraz stacji roboczej.

Podczas tworzenia specjalnej kolejki wyjściowej można określić kilka parametrów dotyczących ochrony:

- **parametr Wyświetlanie danych (Display Data - DSPDTA)**: parametr DSPDTA określa, czy użytkownik może przeglądać, wysyłać lub kopiować zbiór buforowy, którego właścicielem jest inny użytkownik,
- **parametr Uprawnienia do sprawdzania (Authority to Check - AUTCHK)**: parametr AUTCHK określa, czy użytkownik może zmieniać lub usuwać zbiór buforowy, który posiada inny użytkownik,
- **parametr Sterowane przez operatora (Operator Control - OPRCTL)**: parametr OPRCTL określa, czy użytkownicy z uprawnieniem specjalnym *JOBCTL (lub klasa użytkownika *SYSOPR) mogą sterować kolejką wyjściową.

Parametry kolejki wyjściowej, uprawnienia użytkownika dotyczące kolejki wyjściowej oraz uprawnienia specjalne użytkownika współdziałają ze sobą, w celu określenia które funkcje użytkownik może wykonywać na zbiorze buforowym w kolejce wyjściowej. Poniższa tabela pokazuje, które kombinacje umożliwiają użytkownikom wykonywanie różnych funkcji:

Funkcje drukowania	Parametr kolejki wyjściowej			Uprawnienia do kolejki wyjściowej	Uprawnienia specjalne
	DSPDTA	**AUTCHK**	**OPRCTL**		
Dodawanie do kolejki zbioru buforowego[1]	Any (dowolna)	Any (dowolna)	Any (dowolna)	*READ	brak
	Any (dowolna)	Any (dowolna)	*Yes	Any (dowolna)	*JOBCTL
Przeglądanie listy zbiorów buforowych (komenda WRKOUTQ)[2]	Any (dowolna)	Any (dowolna)	Any (dowolna)	*READ	brak
	Any (dowolna)	Any (dowolna)	*Yes	Any (dowolna)	*JOBCTL
Wyświetlanie, kopiowanie lub wysyłanie zbiorów buforowych (DSPSPLF, CPYSPFL, SNDNETSPLF, SNTCPSPLF)[2]	*YES	Any (dowolna)	Any (dowolna)	*READ	brak
	*NO	*DTAAUT	Any (dowolna)	*CHANGE	brak
	*NO	*OWNER	Any (dowolna)	Owner (Właściciel)[3]	brak
	*YES	Any (dowolna)	*Yes	Any (dowolna)	*JOBCTL
	*NO	Any (dowolna)	*Yes	Any (dowolna)	*JOBCTL
	*OWNER[5]	Any (dowolna)	Any (dowolna)	Any (dowolna)	Any (dowolna)
Zmienianie, usuwanie, wstrzymywanie, zwalnianie zbioru buforowego (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF)[2]	Any (dowolna)	*DTAAUT	Any (dowolna)	*CHANGE	brak
	Any (dowolna)	*OWNER	Any (dowolna)	Owner (Właściciel)[3]	brak
Zmienianie, usuwanie zawartości, wstrzymywanie i zwalnianie kolejki wyjściowej (CHGOUTQ, CLROUTO, HLDOUTQ, RLSOUT)[2]	Any (dowolna)	*DTAAUT	Any (dowolna)	*CHANGE	brak
	Any (dowolna)	*OWNER	Any (dowolna)	Owner (Właściciel)[3]	brak
	Any (dowolna)	Any (dowolna)	*YES	Any (dowolna)	*JOBCTL
Uruchamianie programu piszącego dla kolejki (STRPRTWTR, STRRMTWTR)[2]	Any (dowolna)	*DTAAUT	*Any	*CHANGE[4]	brak
	Any (dowolna)	Any (dowolna)	*YES	Any (dowolna)[4]	*JOBCTL

1 Jest to uprawnienie wymagane do kierowania wydruków do kolejki wyjściowej.

2 Na ekranie należy używać tych komend lub odpowiadających im opcji.

3 Użytkownik musi być właścicielem kolejki wyjściowej.

4 Wymaga także uprawnień *USE do opisu drukarki.

5 Aby pracować z tą komendą, użytkownik musi być właścicielem zbioru buforowego lub mieć uprawnienia specjalne *SPLCTL.

Należy przejrzeć część Planu ochrony fizycznej dotyczącą drukarek. Należy także wypełnić sekcję Formularza ochrony zbiorów wydruków oraz stacji roboczej, która dotyczy kolejki wyjściowej.

Przed zaplanowaniem ochrony zasobów stacji roboczych warto zapoznać się z przykładem, w którym Sharon Jones z przedsiębiorstwa JKL Toy określiła wartości dla parametrów kolejki wyjściowej.

Przykład: Formularz ochrony kolejki wyjściowej i stacji roboczej dla przedsiębiorstwa JKL Toy — część dotycząca kolejki wyjściowej

Dział sprzedaży i marketingu przedsiębiorstwa JKL Toy ma dwa wymagania dotyczące poufnych wydruków:

- podstawowe listy płac drukowane są kiedy planuje się zmiany płac; nikt spoza działu sprzedaży i marketingu, poza menedżerami przedsiębiorstwa, nie może zobaczyć tych informacji,
- podczas negocjowania kontraktów, są one poufne; wstępny szkic kontraktu może być przeglądany tylko przez osobę, która go negocjuje, a nie przez pozostałych członków działu sprzedaży i marketingu.

Sharon zadecydowała o utworzeniu dwóch specjalnych kolejek wyjściowych:

PRICEQ
Do użycia dla podstawowych list płac. Na tej kolejce wyjściowej funkcje może wykonywać każda osoba z działu sprzedaży i marketingu. Nikt spoza działu, z wyjątkiem operatorów systemu, nie może używać tej kolejki. Kolejka PRICEQ znajduje się w bibliotece KONTRAKTY.

NEWCP
Do drukowania kontraktów, które są negocjowane. Kolejka wyjściowa jest współużytkowanaa przez członków działu sprzedaży i marketingu, ale tylko osoba, która utworzyła zbiór buforowy, może go kontrolować. Kolejka NEWCP znajduje się w bibliotece KONTRAKTY.

Przedstawiona poniżej tabela prezentuje Formularz ochrony kolejki wyjściowej i stacji roboczej, który Sharon przygotowała dla tych kolejek wyjściowych:

Tabela 54. Formularz ochrony kolejki wyjściowej i stacji roboczej dla przedsiębiorstwa JKL Toy: przykład kolejki wyjściowej wydruku

Lista parametrów dla ograniczonych kolejek wyjściowych:				
Nazwa kolejki wyjściowej	Biblioteka kolejki wyjściowej	Wyświetlenie dowolnego zbioru (Display Any File - DSPDTA)	Uprawnienia do sprawdzania (Authority to Check - AUTCHK)	Sterowane przez operatora (Operator Control - OPRCTL)
PRICEQ	KONTRAKTY	*YES	*DTAAUT	*NO
NEWCP	KONTRAKTY	*NO	*OWNER	*NO

Temat Decydowanie o uprawnieniach publicznych do bibliotek programów zawiera przykład prezentujący uprawnienia do biblioteki KONTRAKTY w przedsiębiorstwie JKL Toy. Dostęp do tej biblioteki mają tylko menedżerowie i członkowie działu sprzedaży i marketingu. Uprawnienia publiczne dla obiektów w tej bibliotece (włączając w to kolejki wyjściowe) to *CHANGE.

Ponieważ parametr AUTCHK kolejki wyjściowej NEWCP ma wartość *OWNER, ze zbiorem buforowym może pracować tylko właściciel tego zbioru (patrz kolumna Wymagane uprawnienia do wykonywania funkcji drukowania w powyższej tabeli). Zapobiega to drukowaniu lub przeglądaniu nowych kontraktów w kolejce wyjściowej przez innych członków działu sprzedaży i marketingu.

Po zaplanowaniu ochrony kolejki wyjściowej wydruków można zaplanować ochronę stacji roboczych.

Planowanie ochrony stacji roboczych

Po zaplanowaniu ochrony zasobów dotyczącej drukarek i zbiorów wydruków można rozpocząć planowanie ochrony stacji roboczej. W Planie ochrony fizycznej wymieniono stacje robocze jako elementy, które mogą stanowić zagrożenie ochrony z powodu ich umiejscowienia. Te informacje pomogą określić, na które stacje robocze należy nałożyć ograniczenia.

Użytkownicy korzystający z tych stacji roboczych powinni stosować szczególną ochronę. Powinni wypisywać się za każdym razem, gdy odchodzą od swojej stacji roboczej. W strategii ochrony można zapisać swoje decyzje dotyczące procedur wypisywania się z niektórych stacji roboczych. W celu zminimalizowania niebezpieczeństwa można także ograniczyć funkcje, które mogą być wykonywane na takich stacjach roboczych.

Najłatwiejszą metodą ograniczania funkcji jest ich ograniczenie do profili użytkowników z ograniczonymi funkcjami. Sharon Jones korzysta z tej techniki w przypadku magazynu przedsiębiorstwa JKL Toy. Pracownikom rampy załadowczej, czyli Rayowi Wagnerowi i Janice Ames, umożliwiła uruchamianie tylko programu przyjmowania towarów. Są to także jedyni użytkownicy, którzy mogą wpisywać się do stacji roboczej na rampie załadowczej.

Można także umożliwić wpisywanie się do każdej stacji roboczej osób z uprawnieniami szefa ochrony lub uprawnieniami serwisowymi. Jeśli w tym celu użyta zostanie wartość systemowa QLMTSECOFR, osoby z uprawnieniami szefa ochrony będą mogły wpisywać się tylko do autoryzowanych stacji roboczych.

Należy przygotować część Formularza ochrony kolejki wyjściowej i stacji roboczej, która dotyczy stacji roboczych.

Po przygotowaniu tej części można zapoznać się z przykładem przedstawiającym sposób planowania ochrony stacji roboczych przez Sharon. Aby upewnić się, że plan ochrony zasobów jest prosty i kompletny, należy także przejrzeć listę zaleceń dotyczącą ochrony zasobów. Po zapoznaniu się z przykładem i zaleceniami, można rozpocząć planowanie instalowania aplikacji.

Przykład: Formularz ochrony kolejki wyjściowej i stacji roboczej dla przedsiębiorstwa JKL Toy — część dotycząca stacji roboczej

Sharon Jones przejrzała swój plan ochrony fizycznej, aby określić które stacje robocze narażone są na ryzyko związane z ochroną. W przedsiębiorstwie JKL Toy osoby spoza firmy łatwo mogą uzyskać dostęp do stacji roboczych na rampie załadowczej oraz w zdalnych biurach sprzedaży. Na planie ochrony fizycznej Sharon wskazała, że te stacje robocze są narażone na ryzyko związane z ochroną.

Najłatwiejszą metodą ograniczania funkcji jest ich ograniczenie do profili użytkowników z ograniczonymi funkcjami. Sharon Jones korzysta z tej techniki w przypadku magazynu przedsiębiorstwa JKL Toy. Pracownikom rampy załadowczej, czyli Rayowi Wagnerowi i Janice Ames, umożliwiła uruchamianie tylko programu przyjmowania towarów. Są to także jedyni użytkownicy, którzy mogą wpisywać się do stacji roboczej na rampie załadowczej.

Sharon ponownie oceniła swój wybór dla wartości systemowej QLMTSECOFR. Zadecydowała, że ustawi ją na 1(Tak - Yes) jako dodatkowe zabezpieczenie narażonych stacji roboczych, które znajdują się na rampie załadowczej i w zdalnych biurach sprzedaży.

Poniższa tabela prezentuje część dotyczącą stacji roboczej z Formularza ochrony kolejki wyjściowej i stacji roboczej, przygotowanego przez Sharon.

Tabela 55. Formularz ochrony kolejki wyjściowej i stacji roboczej dla przedsiębiorstwa JKL Toy: przykład stacji roboczej

Stacje robocze szefa ochrony: Jeśli szef ochrony ma ograniczony dostęp do określonych stacji roboczych (wartość systemowa QLMTSECOFR ustawiona jest na tak), poniżej należy wymienić stacje robocze autoryzowane dla szefa ochrony oraz użytkowników z uprawnieniami *ALLOBJ: Wszystkie stacje robocze, z wyjątkiem wymienionych poniżej	
Poniżej należy wymienić uprawnienia dla ograniczonych stacji roboczych:	
Nazwa stacji roboczej	Grupy lub użytkownicy, którzy są autoryzowani (uprawnienia *CHANGE)
DSP10	AMESJ, WAGNERR
DSP11	AMESJ, WAGNERR
RMT01	UNGERJ, BELLB
RMT02	UNGERJ, BELLB

Przed zaplanowaniem instalowania aplikacji warto przejrzeć podsumowanie zaleceń dotyczących ochrony zasobów.

Podsumowanie zaleceń dotyczących ochrony zasobów

Po zakończeniu planowania ochrony stacji roboczych warto zapoznać się z poniższymi zaleceniami dotyczącymi ochrony zasobów. System iSeries oferuje wiele opcji zabezpieczających informacje. Umożliwia to elastyczne projektowanie planu ochrony zasobów, który jest najlepszy dla danego przedsiębiorstwa. Ale bogactwo opcji może także wprawiać w zakłopotanie.

Na przykładzie przedsiębiorstwa JKL Toy, w tym temacie spróbowano zademonstrować podstawowe podejście do planowania ochrony zasobów, wykorzystując następujące wskazówki:

- Od ogółu do szczegółu:
  - należy planować ochronę bibliotek; pojedynczymi obiektami należy zająć się tylko w razie konieczności,
  - najpierw należy planować uprawnienia publiczne, po nich uprawnienia grup oraz użytkowników.
- Aby zwiększyć wydajność oraz uprościć składowanie i odtwarzanie, należy zdefiniować określoną ochronę tylko dla obiektów, których wymagania ochrony nie mogą być spełnione przez uprawnienia publiczne.
- Uprawnienia publiczne dla nowych obiektów w bibliotece (CRTAUT) powinny być takie same, jak uprawnienia zdefiniowane dla większości obiektów istniejących w bibliotece.
- Grupom oraz użytkownikom nie należy nadawać mniejszych uprawnień niż uprawnienia publiczne. Takie działanie powoduje zmniejszenie wydajności, może prowadzić do powstawania pomyłek oraz utrudnia kontrolę. Jeśli wiadomo, że wszyscy mają przynajmniej uprawnienia publiczne dla obiektów, planowanie i kontrolowanie ochrony stanie się łatwiejsze.
- Do grupowania obiektów z tymi samymi wymaganiami ochrony należy używać list autoryzacji. Listy autoryzacji są prostsze do zarządzania, niż pojedyncze uprawnienia oraz ułatwiają odtwarzanie informacji o ochronie.
- Właścicielami aplikacji powinny być profile użytkowników utworzone specjalnie w tym celu. Hasło właściciela powinno mieć wartość *NONE.
- Należy unikać nadawania praw własności profilom dostarczanym przez firmę IBM, takim jak QSECOFR lub QPGMR.
- Dla raportów poufnych należy korzystać ze specjalnych kolejek wyjściowych. Kolejkę wyjściową należy umieścić w tej samej bibliotece co informacje poufne.
- Należy ograniczyć listę osób z uprawnieniami szefa ochrony.
- Należy być ostrożnym przy nadawaniu uprawnień *ALL dla obiektów i bibliotek. Osoby z uprawnieniami *ALL mogą przypadkowo je usunąć.

Aby upewnić się, że konfigurowanie ochrony zasobów zostało poprawnie zaplanowane, należy zebrać następujące informacje:

- formularze opisywania biblioteki dla wszystkich bibliotek aplikacji, z wypełnioną częścią 1 i 2,
- formularze pojedynczego profilu użytkownika z wypełnionymi polami **Właściciel tworzonych obiektów** oraz **Uprawnienia grupy do tworzonych obiektów**,
- formularz konwencji nazewnictwa z opisem planu nazewnictwa list autoryzacji,
- formularz listy autoryzacji,
- formularz opisywania biblioteki z dodanymi informacjami na temat list autoryzacji,
- formularz ochrony kolejki wyjściowej i stacji roboczej.

Teraz można zaplanować instalowanie aplikacji.

Planowanie instalowania aplikacji

Aby zakończyć planowanie ochrony zasobów, należy przygotować instalowanie aplikacji. Poniższe tematy pomogą w zaplanowaniu praw własności oraz uprawnień do aplikacji po ich zainstalowaniu. Opisane tutaj metody mogą nie być skuteczne dla niektórych aplikacji. Aby stworzyć dobry plan instalowania, należy skonsultować się z programistą lub dostawcą aplikacji.

Jeśli planowany jest zakup aplikacji od dostawcy, należy skorzystać z tych informacji, aby zaplanować czynności dotyczące ochrony, które należy wykonać przed i po załadowaniu bibliotek aplikacji.

Jeśli planuje się instalowanie aplikacji napisanej przez programistę w systemie użytkownika, należy skorzystać z tych informacji, aby zaplanować czynności dotyczące ochrony, które należy wykonać podczas przenoszenia aplikacji ze stanu testowania do produkcyjnego.

Poniższe czynności należy wykonać dla jednej aplikacji. Następnie należy powrócić do tego miejsca i przygotować Formularze instalowania aplikacji dla dodatkowych aplikacji.

Które formularze są potrzebne?

Należy wykonać kopię poniższych formularzy i wypełniać je w czasie pracy z tym tematem:

Tabela 56. Formularze planowania potrzebne do zaplanowania instalowania aplikacji

Nazwa formularza	Potrzebna liczba kopii
Formularz instalowania aplikacji	Jeden na każdą aplikację

Aby zebrać informacje dotyczące planowania instalowania aplikacji, należy skorzystać z formularzy, z którymi pracowano wcześniej:

Nazwa formularza	Przygotowany w:
Formularz opisywania biblioteki	Opisywanie informacji dotyczących bibliotek
Formularz list autoryzacji	Grupowanie obiektów

W temacie Ładowanie aplikacji zawarto informacje dotyczące wykonywania czynności potrzebnych do zainstalowania aplikacji.

Przed planowaniem instalowania aplikacji należy zapoznać się z następującymi tematami:

- Określanie profili użytkowników oraz wartości instalacyjnych dla aplikacji.
- Zmienianie wartości instalacyjnych.

Określanie profili użytkowników oraz wartości instalacyjnych dla aplikacji.

Podczas planowania instalowania aplikacji dla każdej aplikacji należy najpierw wybrać profile użytkowników oraz wartości instalacyjne. Przed zainstalowaniem aplikacji, które zostały utworzone w innym systemie, konieczne może być utworzenie jednego lub więcej profili użytkowników. Przed załadowaniem bibliotek w systemie powinien istnieć profil użytkownika, który ma prawa własności do bibliotek i obiektów aplikacji. Na Formularzu instalowania aplikacji należy zapisać profile, które należy utworzyć dla każdej biblioteki oraz wymagane przez nie parametry.

Aby określić wymagane wartości instalacyjne, programiście lub dostawcy aplikacji należy zadać przedstawione poniżej pytania, a odpowiedzi zapisać w Formularzu instalowania aplikacji:

- Który profil ma prawa własności do biblioteki aplikacji?
- Który profil ma prawa własności do obiektu w bibliotece?
- Jakie uprawnienia publiczne wymagane są do biblioteki (AUT)?
- Jakie uprawnienia publiczne wymagane są do nowych obiektów (CRTAUT)?
- Jakie uprawnienia publiczne wymagane są do obiektów w bibliotece?
- Jakie programy, jeśli takie są, adoptują uprawnienia właściciela?

Należy dowiedzieć się, czy programiści lub dostawca aplikacji utworzyli jakiekolwiek listy autoryzacji dla aplikacji. Dla każdej utworzonej listy autoryzacji należy przygotować Formularz list autoryzacji lub poprosić programistę o informacje na temat listy.

Teraz można określić, czy należy zmienić wartości instalacyjne.

Zmienianie wartości instalacyjnych dla aplikacji

Informacje z Formularza instalowania aplikacji należy porównać z planem ochrony zasobów dla biblioteki, zawartym w Formularzu opisywania biblioteki. Jeśli są różne, należy zadecydować, jakie zmiany należy wprowadzić po zainstalowaniu aplikacji.

Zmienianie prawa własności do aplikacji

Jeśli programista lub dostawca aplikacji utworzył specjalny profil, który ma prawa własności do bibliotek i obiektów aplikacji, należy rozważyć używanie tego profilu, nawet jeśli nie pasuje do wybranej konwencji nazewnictwa. Przenoszenie prawa własności dla obiektów może zająć dużo czasu i należy go unikać.

Jeśli jeden z profili grupowych dostarczanych przez firmę IBM, na przykład QSECOFR lub QPGMR, ma prawa własności do aplikacji, po zainstalowaniu aplikacji te prawa należy przenieść na inny profil.

Czasami programiści tak projektują aplikacje, aby zapobiec zmianie praw własności do obiektu. Należy spróbować zmienić te ograniczenia tak, aby spełniły wymagania dotyczące zarządzania ochroną. Jednak jeśli profile dostarczane przez firmę IBM, takie jak QSECOFR, mają prawa własności do aplikacji, użytkownik oraz programista lub dostawca aplikacji muszą opracować plan zmiany praw własności. Najlepszym rozwiązaniem jest zmiana praw własności przed zainstalowaniem aplikacji.

Zmienianie uprawnień publicznych

Podczas składowania obiektu składowane są także uprawnienia publiczne do niego. Po odtworzeniu w systemie biblioteki aplikacji, biblioteka oraz wszystkie jej obiekty będą miały takie same uprawnienia publiczne, jakie miały podczas składowania. Dzieje się tak nawet w przypadku składowania biblioteki w innym systemie.

Wartość CRTAUT dla biblioteki (uprawnienia publiczne dla nowych obiektów) nie wpływa na odtwarzane obiekty. Są one odtwarzane w zachowanymi uprawnieniami publicznymi, niezależnie od wartości CRTAUT dla biblioteki.

Uprawnienia publiczne do bibliotek i obiektów należy zmienić tak, aby były zgodne z planem zapisanym w Formularzu opisywania biblioteki.

Podczas planowania instalowania aplikacji warto zapoznać się z przykładem pokazującym, w jaki sposób Sharon Jones z przedsiębiorstwa JKL Toy zaplanowała instalowanie aplikacji.

Aby upewnić się, że instalowanie aplikacji zostało dobrze zaplanowane, należy:

- zakończyć wypełnianie początkowego Formularza instalowania aplikacji; następnie wrócić do tego miejsca i przygotować formularze dla każdej dodatkowej aplikacji,
- przejrzeć wszystkie formularze i upewnić się, że zostały wypełnione; wykonać ich kopie i schować w bezpiecznym miejscu, do czasu zainstalowania systemu oraz programów licencjonowanych.

Po wykonaniu tych zadań planowania, można skonfigurować ochronę użytkowników.

Przykład: Formularz instalowania aplikacji dla przedsiębiorstwa JKL Toy: Przedsiębiorstwo JKL Toy zakupiło aplikacje Zamówienia klientów oraz Należności od dostawcy aplikacji. Zatrudniło także programistę, aby stworzył aplikację Kontrakty i wycena oraz powiązał ją z aplikacją Zamówienia klientów.

Sharon Jones wykorzystała informacje z Formularzy opisywania bibliotek do przygotowania Formularza instalowania aplikacji. Poniższa tabela prezentuje kopię Formularza opisywania biblioteki przygotowanego przez Sharon dla biblioteki CUSTLIB: (informacje na ten temat zawiera sekcja ″Opisywanie informacji dotyczących bibliotek″).

Tabela 57. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład

Formularz opisywania biblioteki	**Część 1 z 2**

Tabela 57. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy: przykład (kontynuacja)

Przygotowany przez: Sharon Jones	Data: 9/9/99
Nazwa biblioteki: CUSTLIB	Nazwa opisowa (tekst): Biblioteka klientów
Krótki opis funkcji tej biblioteki: Przechowuje wszystkie pliki klientów, w tym zamówienia i należności.	

Zdefiniowane cele ochrony biblioteki, określające czy zawiera poufne informacje:
`Obecnie każda osoba w przedsiębiorstwie może przeglądać zamówienia klientów.`
`Aby zapewnić integralność informacji, należy ograniczyć liczbę osób zmieniających te informacje.`	

Uprawnienia publiczne do biblioteki: *USE Uprawnienia publiczne dla obiektów biblioteki: *CHANGE Uprawnienia publiczne dla nowych obiektów (CRTAUT): *CHANGE Właściciel biblioteki: OWNAR	

Poniższa tabela prezentuje Formularz instalowania aplikacji, który Sharon przygotowała dla aplikacji Zamówienia klientów. Należy zauważyć, że Sharon zdecydowała się użyć profilu właściciela utworzonego przez dostawcę aplikacji. Profil COWNER będzie właścicielem zarówno plików jak i biblioteki programu.

Po zainstalowaniu aplikacji Sharon powinna wykonać następujące czynności:

- zmienić uprawnienia publiczne dla bibliotek, aby były zgodne z planem ochrony zasobów zapisanym w Formularzu opisywania biblioteki,
- zmienić klasę użytkownika profilu COWNER na wartość *USER i usunąć uprawnienia specjalne,
- zmienić hasło profilu COWNER na wartość *NONE.

Tabela 58. Formularz instalowania aplikacji dla przedsiębiorstwa JKL Toy: przykład

Nazwa aplikacji: Zamówienia klientów (CO)		Opis: Wprowadzanie, śledzenie i dostarczanie zamówień
Lista oraz wyjaśnienie, dlaczego potrzebne są wszystkie profile, które trzeba utworzyć do zainstalowania aplikacji: Biblioteka zawiera pliki, których właścicielem jest profil COWNER. Właścicielem biblioteki programu jest QPGMR.		
Nazwa biblioteki: CUSTLIB		
	Przed zainstalowaniem	**Po zainstalowaniu**
Właściciel biblioteki	COWNER	COWNER
Właściciel obiektu	COWNER	COWNER
Uprawnienia publiczne do biblioteki	*EXCLUDE	*USE
Uprawnienia publiczne dla obiektu	*ALL	*CHANGE
Uprawnienia publiczne dla nowych obiektów	*CHANGE	*CHANGE
Nazwa biblioteki: COPGMLIB		
	Przed zainstalowaniem	**Po zainstalowaniu**
Właściciel biblioteki	QPGMR	COWNER
Właściciel obiektu	QPGMR	COWNER
Uprawnienia publiczne do biblioteki	*EXCLUDE	*USE
Uprawnienia publiczne dla obiektu	*ALL	*CHANGE
Uprawnienia publiczne dla nowych obiektów	*CHANGE	*CHANGE

Po zakończeniu zadań planowania można skonfigurować ochronę użytkowników.

Konfigurowanie ochrony użytkowników

W tym temacie opisano zadania wymagane do skonfigurowania ochrony użytkowników systemu za pomocą interfejsu wiersza komend. W przypadku konfigurowania nowego systemu, należy wykonać kolejno podane czynności. Po przejściu do następnej czynności system korzysta z informacji podanych w poprzednich krokach. Aby skonfigurować podstawową ochronę systemu, należy wykonać dwa zestawy czynności. Najpierw należy zdefiniować ochronę użytkowników, a następnie zabezpieczyć zasoby systemowe. Przedstawione poniżej dwie tabele zawierają wszystkie czynności, które należy wykonać w celu zapewnienia ochrony użytkowników oraz zasobów.

Uwaga: Przed rozpoczęciem konfigurowania ochrony zasobów, najpierw **TRZEBA** wykonać wszystkie czynności dotyczące konfigurowania ochrony użytkowników.

Tabela 59. Czynności wymagane do skonfigurowania ochrony użytkowników

Czynność	Co należy wykonać	Których formularzy należy użyć
Konfigurowanie środowiska ogólnego	Konfigurowanie początkowych wartości systemowych oraz atrybutów sieciowych. Tworzenie profilu użytkownika dla szefa ochrony.	Formularz wybierania wartości systemowych
Ustawianie wartości systemowych dotyczących ochrony	Konfigurowanie dodatkowych wartości systemowych.	Formularz wybierania wartości systemowych
Przygotowywanie czynności podstawowej ochrony systemu dla ładowania aplikacji	Tworzenie profili właścicieli. Ładowanie aplikacji. Przed zakończeniem pozostałych czynności, w systemie muszą znajdować się biblioteki i obiekty aplikacji.	Formularz instalowania aplikacji
Konfigurowanie grup użytkowników	Tworzenie opisów zadań, bibliotek dla grup oraz profili grupowych.	Formularz opisywania grupy użytkowników
Konfigurowanie pojedynczych użytkowników	Tworzenie pojedynczych bibliotek oraz profili użytkowników.	Formularz pojedynczego profilu użytkownika

Tabela 60. Czynności wymagane do skonfigurowania ochrony zasobów

Czynność	Co należy wykonać	Których formularzy należy użyć
Ustawianie praw własności oraz uprawnień publicznych	Ustanawianie praw własności oraz uprawnień publicznych do bibliotek i obiektów.	Formularz instalowania aplikacji
Tworzenie list autoryzacji	Tworzenie list autoryzacji.	Formularz list autoryzacji
Konfigurowanie określonych uprawnień	Konfigurowanie dostępu do bibliotek i pojedynczych obiektów.	Formularz opisywania biblioteki
Zabezpieczanie zbiorów wydruków	Zabezpieczanie zbiorów wydruków poprzez tworzenie kolejek wyjściowych oraz przypisywanie wydruków.	Formularz ochrony kolejki wyjściowej i stacji roboczej
Zabezpieczanie stacji roboczych	Zabezpieczanie stacji roboczych.	Formularz ochrony kolejki wyjściowej i stacji roboczej

Oprócz tematów wymienionych w powyższej tabeli, należy zapoznać się także z następującymi tematami dotyczącymi zarządzania ochroną systemu:

- Testowanie ochrony.
- Zmienianie informacji o ochronie.
- Składowanie informacji o ochronie.
- Monitorowanie ochrony.

Zanim zaczniesz

W przypadku instalowania nowego systemu, przed rozpoczęciem konfigurowania ochrony należy wykonać następujące czynności:

- upewnij się, że jednostka systemowa oraz urządzenia są zainstalowane i działają poprawnie; Jeśli nie planuje się korzystania z konwencji nazewnictwa systemu iSeries dla urządzeń, po zmianie wartości systemowych, które określają sposób nazewnictwa urządzeń (QDEVNAMING), należy zaczekać na podłączenie stacji roboczych i drukarek. Zastosowanie nowych wartości systemowych powiadamia kiedy podłączyć urządzenia,
- załaduj wszystkie programy licencjonowane, które mają być używane.

Ogólne konfigurowanie środowiska

Aby rozpocząć konfigurowanie ochrony użytkowników, należy skonfigurować środowisko ogólne dla użytkowników. W tym temacie do ustawienia wartości systemowych i utworzenia własnego profilu użytkownika użyte zostanie menu menu SETUP. Zmianie ulegną także identyfikatory użytkowników oraz hasła profili dla narzędzi DST.

W poniższych procedurach będzie można napotkać przykłady ekranów wiersza komend, które ilustrują wykonywane czynności. Jednak nie prezentują one zawartości całego ekranu. Przedstawiają tylko informacje, które są wymagane do zakończenia zadania.

Które formularze są potrzebne?

Informacje z Formularza wybierania wartości systemowych, który został przygotowany w sekcji ″Planowanie ogólnej strategii ochrony.″

Aby skonfigurować środowisko ogólne, należy wykonać następujące zadania:

1. Wpisywanie się do systemu.
2. Wybieranie odpowiedniego poziomu asysty.
3. Zapobieganie wpisywaniu się innych użytkowników.
4. Podawanie wartości systemowych dotyczących ochrony.
5. Stosowanie nowych wartości systemowych.
6. Tworzenie profilu szefa ochrony

Po wykonaniu powyższych czynności trzeba będzie zmienić hasła narzędzi serwisowych, aby zabezpieczyć się przed ich nieodpowiednim użyciem. Więcej szczegółów na ten temat zawiera sekcja Narzędzia serwisowe.

Wpisywanie się do systemu

Aby rozpocząć konfigurowanie środowiska systemu, należy wpisać się do niego.

1. Z poziomu konsoli wpisz się jako szef ochrony (QSECOFR). Jeśli wpisywanie odbywa się po raz pierwszy, wpisz hasło QSECOFR. Ponieważ system dostarczany jest z hasłem, które utraciło ważność, użytkownik zostanie poproszony o zmianę tego hasła. Aby pomyślnie wpisać się do systemu, należy zmienić to hasło.
2. Na ekranie Wpisywanie się w polu *Menu* wpisz SETUP.

Uwaga: menu SETUP wywoła menu Dostosowanie systemu, użytkowników i urządzeń (Customize Your System, Users, and Devices). W tym tekście nazywane jest ono menu SETUP.

```
                Wpisanie się (Sign On)
                            System  . . . . .
                            Podsystem . . . .
                            Ekran . . . . . .

Użytkownik. . . . . .  .  .  QSECOFR
Hasło . . . . . .  .  .  .  .  _________
Program/procedura . . . . . .  _________
Menu  . . . . . .  .  .  .  .  SETUP
Biblioteka bieżąca. . . . . .  _________
```

Po wpisaniu się do systemu należy wybrać odpowiedni poziom asysty.

Wybieranie odpowiedniego poziomu asysty

Po wpisaniu się do systemu można wybrać odpowiedni poziom asysty dla użytkowników. **Poziom asysty** określa widzianą przez użytkownika wersję ekranu. Wiele ekranów systemowych ma dwie różne wersje:

- wersję podstawowy poziom asysty, która zawiera mniej informacji i nie korzysta z terminologii technicznej,
- wersję intermediate assistance level, która prezentuje więcej informacji i korzysta z terminów technicznych.

Niektóre pola lub funkcje dostępne są tylko w odpowiedniej wersji ekranu. Instrukcje informują, której wersji należy użyć. Aby zmienić poziom asysty na inny, należy nacisnąć klawisz **F21** (Wybór poziomu asysty). Klawisz **F21** nie jest dostępny na wszystkich ekranach.

Po wybraniu poziomu asysty należy zabezpieczyć się przed wpisywaniem się innych użytkowników do systemu podczas konfigurowania ochrony.

Zabezpieczanie się przed wpisywaniem się innych użytkowników

Po wybraniu odpowiedniego poziomu asysty, należy zablokować możliwość wpisania się do systemu przez innych użytkowników. Jeśli istnieje obawa przed ingerencją osób nieuprawnionych zanim system zostanie zabezpieczony, można zapobiec wpisywaniu się z innych stacji roboczych. Jest to czynność opcjonalna. Należy ją wykonać tylko wtedy, gdy konieczna jest tymczasowa ochrona:

1. W menu menu SETUP naciśnij klawisz **F9**, aby wyświetlić wiersz komend.
2. W wierszu komend wpisz GO DEVICESTS.
3. Ekran zaprezentuje menu Zadania związane ze statusem urządzeń (Device Status Tasks). Jeśli pojawi się menu Praca ze statusem konfiguracji (Work with Configuration Status), naciśnij klawisz **F21** (Wybór poziomu asysty), aby zmienić podstawowy poziom asysty.
4. Wybierz opcję **1** (Praca z terminalami).
5. Na ekranie Praca z terminalami (Work with Display Devices) zablokuj wszystkie stacje robocze, z wyjątkiem tej na której pracujesz. Można to zrobić wpisując **2** obok nazwy każdej stacji roboczej i naciskając klawisz **Enter**.
6. Naciskając dwa razy klawisz **F3** (Wyjdź), wróć do menu menu SETUP.
7. Aby usunąć wiersz komend, naciśnij klawisz **F12** (Anuluj).

```
                  Praca z terminalami
               (Work with Display Devices)

 Wpisz opcje i naciśnij klawisz Enter.
  1=Udostępnij          2=Zablokuj        5=Wyświetl
  7=Wyświetl komunikat  8=Praca z kontrolerem i linią
  13=Zmień opis

Opc  Urządz.     Typ     Status
__   DSP01       3196    QSECOFR
2_   DSP02       3196    Dostępne do użycia
2_   DSP03       3196    Dostępne do użycia
2_   DSP04       3196    Dostępne do użycia
```

Po zablokowaniu urządzenia, nie pojawi się ekran wpisywania się, nawet jeśli zostanie ono włączone. Stacje robocze będą niedostępne tylko do czasu zatrzymania i ponownego uruchomienia systemu. Konieczne może być powtórzenie tej czynności.

Po zabezpieczeniu się przed wpisaniem się do systemu, można podać wartości systemowe dotyczące ochrony.

Podawanie wartości systemowych dotyczących ochrony

Po zabezpieczeniu się przed wpisaniem się innych użytkowników należy podać wartości systemowe.

Poniższa procedura umożliwia wpisanie informacji z części 1 Formularza wybierania wartości systemowych:

1. W menu menu SETUP wybierz opcję **1** (Zmiana opcji systemu).
2. Na ekranie Zmiana opcji systemu (Change System Options) wpisz informacje z Formularza wybierania wartości systemowych. Jeśli nie chcesz zmieniać jakiejś wartości, naciśnij klawisz Tab, aby przejść dalej.
3. Jeśli nie zrobiono tego podczas uruchamiania systemu, wpisz na ekranie poprawną datę i godzinę.
4. Po wpisaniu informacji na danej stronie, przejdź do następnej. Napis *Więcej...* w prawym dolnym rogu ekranu oznacza, że ekran ma więcej niż jedną stronę.

```
                          Zmiana opcji systemu
                        (Change System Options)
System:
Wpisz opcje i naciśnij klawisz Enter.

Nazwa systemu . . . . . .   JKLTOY     Nazwa

Opcje daty i czasu:
  Data systemowa. . . . . .   09/21/99     MM/DD/YY
  Czas systemowy. . . . . .   10:52:57     HH:MM:SS
  Separator daty  . . . . .   1            1=/
                                           2=-
                                           3=.
                                           4=,
                                           5=pusty
  Format daty . . . . . .   MDY            YMD, MDY, DMY, JUL
  Separator czasu . . . . .   1            1=:
                                           2=.
                                           3=,
                                           4=pusty


                                                              Więcej...
F1=Pomoc   F3=Wyjście   F5=Odśwież   F12=Anuluj
```

5. Wpisz wybrane wartości na drugiej stronie ekranu i przejdź do następnej.

```
                          Zmiana opcji systemu
                        (Change System Options)

Wpisz opcje i naciśnij klawisz Enter.

Opcje ochrony:
  Poziom ochrony  . . . . . .   40
   :
  Umożliwienie szefowi ochrony
    wpisywania się na każdej
    stacji roboczej . . . . . .   N
```

6. Wpisz wybrane wartości na trzeciej stronie ekranu i naciśnij klawisz **Enter**.

```
                          Zmiana opcji systemu
                        (Change System Options)

Wpisz opcje i naciśnij klawisz Enter.

Opcje urządzeń:
Format nazewnictwa dla nowych
   urządzeń . . . . . .   1


  Systemowa drukasrka domyślna.   PRT01

Opcje dodatkowe:
  Umożliwienie wpisywania się
    w środowisku S/36 . . . . .   N
  Zachowanie informacji
  rozliczeniowych po zakończeniu
    zadań drukowania. . . . . .   Y
```

7. Powinno pojawić się menu menu SETUP. Należy zwrócić uwagę na komunikat u dołu ekranu: **Wartości systemowe zostały zmienione pomyślnie. Wymagane jest przeprowadzenie IPL** .

   Uwaga: System wymaga przeprowadzenia IPL tylko w przypadku zmiany poziomu ochrony.

Na końcu większości tematów dotyczących zadań systemowych, można znaleźć tabelę opisującą możliwe błędy oraz czynności naprawcze. Można je wykorzystać, jeśli wynik działania będzie inny niż opisany w tym temacie. W tabelach nie opisano wszystkich możliwych problemów. Celem ich autorów byłoudostępnienie wskazówek dotyczących rozwiązywania problemów oraz ułatwienie korzystania z systemu.

Możliwy błąd	Rozwiązanie
Wyświetlane jest menu Menu główne (Main).	Naciśnięto klawisz **F3** (Wyjdź) lub **F12** (Anuluj). Wpisz GO SETUP i spróbuj ponownie.
Widać inny ekran, taki jak Zmiana parametrów czyszczenia (Change Cleanup Options).	W menu menu SETUP wybrano złą opcję. Naciśnij klawisz **F3** (Wróć), aby powrócić do menu i spróbować ponownie.
Po naciśnięciu klawisza **Enter** ponownie pojawia się ekran Zmiana opcji systemu (Change System Options).	U dołu ekranu poszukaj komunikatu o błędzie. Prawdopodobnie wpisano niedozwoloną wartość. Jeśli potrzebne są dodatkowe informacje, należy pamiętać o używaniu klawisza **F1** (Pomoc). Jeśli system ma odtworzyć wszystkie wartości, które były podane przed rozpoczęciem wpisywania, należy użyć klawisza **F5** (Odśwież). Spróbuj ponownie.
Przed wprowadzeniem wszystkich zmian naciśnięto klawisz **Enter**.	Tego ekranu, jeśli konieczna jest zmiana wartości systemowych, można używać dowolną ilość razy. Z menu menu SETUP należy wybrać opcję **1** i wpisać pominięte wartości. **Uwaga: gdy system już działa, bez konsultacji z programistą, nie należy zmieniać poziomu ochrony. Jeśli używany jest program iSeries Access lub system komunikuje się z innym systemem, nie należy także zmieniać nazwy systemu.**
Zamiast przejść do następnej strony, naciśnięto klawisz **Enter**.	Z menu menu SETUP wybierz opcję **1** i przejdź do następnej strony. Wpisz nowe wartości i naciśnij klawisz **Enter**.

Po wprowadzeniu wartości systemowych, należy zastosować nowe wartości systemowe.

Stosowanie nowych wartości systemowych.

Po wprowadzeniu wartości systemowych, należy zastosować niektóre z nich. Większość ze zmian wprowadzonych w wartościach systemowych ma natychmiastowy efekt. Jednak zmiana poziomu ochrony w systemie, wchodzi w życie po zatrzymaniu systemu i uruchomieniu go ponownie. Po sprawdzeniu na ekranie Zmiana opcji systemu (Change System Options), że wszystkie wpisane wartości są poprawne, można zastosować nowe wartości.

Uwaga: Jeśli jeszcze tego nie zrobiono, do systemu należy podłączyć stacje robocze. Podczas uruchamiania systemu są onekonfigurowane automatycznie, za pomocą formatu nazw, który wybrano na ekranie Zmiana opcji systemu (Change System Options).

Przedstawiona poniżej procedura umożliwia zatrzymanie systemu oraz jego ponowne uruchomienie. Podczas startowania systemu stosowane są wartości, które wprowadzono na ekranie Zmiana opcji systemu (Change System Options).

1. Upewnij się, że wpisałeś się w konsoli oraz że nikt nie jest wpisany na żadnej z pozostałych stacji roboczych.
2. Upewnij się, że stacyjka w jednostce procesora jest w pozycji Normal.
3. Z menu menu SETUP wybierz opcję Włączanie i wyłączanie systemu.
4. Wybierz opcję natychmiastowego wyłączenia systemu i włącz go ponownie. Naciśnij klawisz **Enter**.
5. System wyświetli ekran, który żąda potwierdzenia wyłączenia systemu. Naciśnij klawisz **F16** (Potwierdź).

Spowoduje to zatrzymanie systemu, a następnie jego automatyczne uruchomienie. Ekran będzie pusty przez kilka minut. Potem powinien pojawić się ekran Wpisanie Się (Sign On).

Po zastosowaniu nowych wartości systemowych należy utworzyć profil szefa ochrony.

Tworzenie profilu szefa ochrony

Szef ochrony to każdy użytkownik z klasą użytkownika *SECOFR lub uprawnieniami specjalnymi *ALLOBJ i *SECADM.

Po zastosowaniu wartości systemowych należy utworzyć profil użytkownika dla siebie oraz alternatywnego szefa ochrony. W przyszłości podczas wykonywania funkcji szefa ochrony zamiast profilu QSECOFR należy używać swojego profilu.

1. Wpisz się do systemu jako użytkownik QSECOFR i wywołaj menu menu SETUP.

   Należy zauważyć, że nazwa wybranego systemu pojawia się w prawym górnym rogu ekranu Wpisanie Się (Sign On).

```
                Wpisanie się (Sign On)
                           System  . . . . .
                           Podsystem . . . .
                           Ekran . . . . . .

Użytkownik. . . . . . . . . . .   QSECOFR
Hasło . . . . . . . . . . . . .   _________
Program/procedura . . . . . . .   _________
Menu  . . . . . . . . . . . . .   SETUP
Biblioteka bieżąca. . . . . . .   _________
```

2. Z menu menu SETUP wybierz opcję *Praca z rejestrowaniem użytkowników*. Na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment) zostanie wyświetlona lista bieżących profili.

   Uwaga: Jeśli pojawia się ekran Praca z profilem użytkownika (Work with User Profile), należy nacisnąć klawisz **F21** (Wybór poziomu asysty) i zmienić na podstawowy poziom asysty.
3. Aby utworzyć nowy profil, w kolumnie *Opc* (opcja) wpisz **1** (Dodaj), a nazwę profilu w kolumnie *Użytkownik*. Naciśnij klawisz **Enter**.

```
            Praca z rejestrowaniem użytkowników
               (Work with User Enrollment)

 Wpisz opcje i naciśnij klawisz Enter.
  1=Dodaj   2=Zmień   3=Kopiuj   4=Usuń   5=Wyświetl

Opc     Użytkownik         Opis
1       JONESS
QDOC                           Profil użytkownika
QSECOFR                        Profil użytkownika szefa ochrony
```

4. Na ekranie Dodawanie użytkowników (Add User) podaj swoje hasło.
5. W polach przedstawionych na przykładowym ekranie wpisz własne, odpowiednie informacje.
6. Przejdź do następnej strony ekranu.

```
                           Dodawanie użytkowników
                               (Add User)

Wpisz opcje i naciśnij klawisz Enter.

Użytkownik. . . . . .   JONESS
Opis użytkownika  . . .   Jones, Sharon
Hasło . . . . . .   secret
Typ użytkownika . . . . .   *SECOFR
Grupa użytkownika . . . .   *NONE

ograniczenie wiersza kom.   _____
Biblioteka domyślna . . .
Drukarka domyślna . . . .   *WRKSTN
Program początkowy. . . .   *NONE
Biblioteka. . . . . .

Menu początkowe . . . . .
Biblioteka. . . . . .
```

7. Wypełnij drugą stronę ekranu i naciśnij klawisz **Enter**.
8. Sprawdź komunikaty potwierdzenia pojawiające się u dołu ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment).
9. Naciśnij klawisz **F3** (Wyjdź), aby powrócić do menu menu SETUP.

```
                           Dodawanie użytkowników
                               (Add User)

Wpisz opcje i naciśnij klawisz Enter.

program klawisza ATTN . .   *SYSVAL
Biblioteka. . . . . .
```

Możliwy błąd	Rozwiązanie
Przed wpisaniem informacji we wszystkich polach naciśnięto klawisz **Enter**.	Na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment) użyj opcji *Zmiana*, aby zmienić właśnie utworzony profil. Jeśli profil nie pojawi się na liście, naciśnij klawisz **F5** (Odśwież) i przejdź do następnej strony, aby go odszukać.

Po utworzeniu profilu szefa ochrony, należy zmienić identyfikator użytkownika i hasło dla użytkowników narzędzi serwisowych. Informacje na ten temat zawiera sekcja Narzędzia serwisowe w Centrum informacyjnym.

Ustawianie wartości systemowych dotyczących ochrony

W tym temacie do zmiany i wyświetlania wartości systemowych użyto komendy Praca z wartościami systemowymi (Work with System Values - WRKSYSVAL).

Które formularze są potrzebne?

Informacje z Formularza wybierania wartości systemowych, który został przygotowany w sekcji ″Planowanie ogólnej strategii ochrony.″

Aby skonfigurować wartości systemowe, należy wykonać następujące zadania:

1. Zmienianie wartości systemowych dotyczących ochrony.
2. Zmienianie pojedynczych wartości systemowych.

Wpisywanie się do interfejsu wiersza komend

Aby wpisać się do systemu, należy podać następujące informacje:

Profil Własny (wymagane uprawnienia *SECADM i *ALLOBJ)

Menu MAIN (Główne)

Po wpisaniu się można rozpocząć zmienianie wartości systemowych dotyczących ochrony.

Zmienianie wartości systemowych dotyczących ochrony

Po wpisaniu się do systemu, aby wprowadzić wartości systemowe podane w części 2 Formularza wybierania wartości systemowych, należy skorzystać z poniższej procedury.

1. W wierszu komend wpisz WRKSYSVAL *SEC i naciśnij klawisz **Enter**. Parametr *SEC oznacza, że mają pojawić się wartości systemowe związane z ochroną.
2. Na ekranie Praca z wartościami systemowymi (Work with System Values), obok wartości systemowej, którą chcesz zmienić, w kolumnie *Opcja* wpisz **2** (Zmiana). Jeśli wartość systemowa, którą chcesz zmienić, nie pojawia się na ekranie, przejdź do następnej strony.

```
                Praca z wartościami systemowymi
                   (Work with System Values)

Ustaw na . . . . . .              Pierwszy znak
Podzbiór wg typu . . . .  *SEC    F4 dla listy

Wpisz opcje i naciśnij klawisz Enter.
  2=Zmień   5=Wyświetl

         Wartość
Opcja    systemowa  Typ         Opis
        QINACTMSGQ  *SEC        Kolejka zadań nieaktywnych
2       QLMTDEVSSN  *SEC        Limit sesji urządzeń
        QLMTSECOFR  *SEC        Limit urządzeń dla szefa ochrony
        QMAXSGNACN  *SEC        Działanie po błędnym wpisaniu się
   ⋮
```

3. Wpisz zmienioną wartość systemową i naciśnij klawisz **Enter**. Ekran Praca z wartościami systemowymi (Work with System Values) zostanie wyświetlony ponownie.

```
              Zmiana wartości systemowych
                (Change System Value)
Wartość systemowa. . . :    QLMTDEVSSN
Opis . . . . . :    Limit sesju urządzeń


Wypełnij pola i naciśnij Enter

  Limit sesji urządzeń . . . .   0          0=Do not
                                            1=Limit
```

4. Sprawdź komunikat potwierdzający, który pojawił się u dołu ekranu.

Możliwy błąd	Rozwiązanie
Widać na nim inne wartości systemowe niż wartości naprzykładowym ekranie Praca z wartościami systemowymi (Work with System Values).	Nie podano parametru *SEC. Porównaj znajdujące się u góry ekranu pole *Subset by type* (Podzbiór według typu) z przykładem. Przesuń kursor na pole *Subset by type* (Podzbiór według typu). Wpisz *SEC i naciśnij klawisz **Enter**.
System nie wykonał komendy. Nadal widać menu.	Sprawdź komunikaty o błędach pojawiające się u dołu ekranu. Prawdopodobnie wpisano nieprawidłową nazwę komendy. Spróbuj ponownie. Jeśli komunikat informuje, że użytkownik nie jest uprawniony, wypisz się i wpisz ponownie za pomocą profilu z uprawnieniami szefa ochrony.
Po naciśnięciu klawisza **Enter** ponownie pojawia się ekran Zmiana wartości systemowych (Change System Value).	Sprawdź dół ekranu w poszukiwaniu komunikatów o błędach. Prawdopodobnie nieprawidłowo wpisano nową wartość lub jest ona spoza dozwolonego zakresu. Dodatkowe informacje można uzyskać po naciśnięciu klawisza **F1** (Pomoc).
Zamiast ekranu Praca z wartościami systemowymi (Work with System Values) widać menu.	Prawdopodobnie dwa razy naciśnięto klawisz **Enter**. Wpisz WRKSYSVAL *SEC.
Wybrano wartość systemową, która nie ma być zmieniana.	Aby powrócić do ekranu Praca z wartościami systemowymi (Work with System Values) naciśnij klawisz **F12** (Anuluj).

Co oznacza * (gwiazdka)?

Prawdopodobnie użytkownik zauważył, że niektóre wartości mają przed sobą gwiazdkę (*). System korzysta z gwiazdki do odróżnienia wartości specjalnych od zwykłych wyrazów. Na przykład podanie wartości *NONE dla hasła profilu użytkownika oznacza, że system uniemożliwi wpisywanie się za pomocą tego profilu. Jeśli podana zostanie wartość NONE, użytkownik musi wpisać znaki NONE jako hasło.

Podczas konfigurowania ochrony systemu, należy zwracać uwagę na używanie gwiazdki w instrukcjach oraz w formularzach.

Po zmianie wartości systemowych dotyczących ochrony, można zmienić pojedyncze wartości systemowe.

Zmienianie pojedynczych wartości systemowych

Po zmianie wartości systemowych dotyczących ochrony, można zmienić pojedyncze wartości systemowe.

Na przykład wartość systemowa interwał czasowy przed przerwaniem odłączonych zadań (QDSCJOBITV) nie jest wartością systemową dotyczącą ochrony. Nie pojawia się na ekranie Praca z wart. systemowymi (Work with System values) w podzbiorze *SEC. Przedstawiona poniżej procedura umożliwia zmianę wartości systemowej QDSCJOBITV lub innej pojedynczej wartości:

1. Wpisz WRKSYSVAL QDSCJOBITV i naciśnij klawisz **Enter**.
2. Na ekranie Praca z wartościami systemowymi (Work with System Values) obok wartości systemowej QDSCJOBITV, w kolumnie *Opcja*, wpisz **2** (Zmień).

3. Wpisz nową wartość QDSCJOBITV.
4. Sprawdź komunikat potwierdzający.

```
               Zmiana wartości systemowych
                 (Change System Value)
Wartość systemowa . . . . . :   QDSCJOBITV
Opis . . . . . :   Interwał czasowy przed przerwaniem odłączonych zadań


Wypełnij pola i naciśnij Enter

Interwał czasowy przed przerwaniem odł. zadań ...... 300
```

Listing wartości systemowych

Po podaniu wszystkich informacji z Formularza wybierania wartości systemowych można wydrukować listę wszystkich wartości systemowych. W tym celu należy wpisać WRKSYSVAL *SEC OUTPUT(*PRINT). Kopię listy należy porównać z Formularzem wybierania wartości systemowych. Po każdej zmianie wartości systemowych należy ponownie wydrukować listę.

Po wprowadzeniu z Formularza wybierania wartości systemowych nowych wartości systemowych można przygotować ładowanie aplikacji.

Przygotowywanie czynności dotyczących ochrony dla ładowania aplikacji

Po ustawieniu wartości systemowych można przygotować ładowanie aplikacji. W tym temacie opisano czynności dotyczące ochrony, które należy wykonać podczasładowania do systemu bibliotek aplikacji. Po utworzeniu profili oraz innych obiektów ochrony, w sekcjach ″Konfigurowanie praw własności i uprawnień publicznych″ oraz ″Konfigurowanie ochrony zasobów″ pokazano sposób nadawania praw własności i uprawnień do aplikacji.

Jeśli to możliwe, biblioteki aplikacji powinny być załadowane do systemu przed skonfigurowaniem grup użytkowników i pojedynczych profili. Podczas tworzenia opisów zadań i profili konieczne jest odniesienie do obiektów aplikacji.

Jeśli załadowanie aplikacji przed utworzeniem profili grupowych i indywidualnych nie jest możliwe, mogą pojawić się komunikaty ostrzegawcze, takie jak następujące:

- The system does not find initial libraries when you create job descriptions (Podczas tworzenia opisów zadań system nie odnalazł bibliotek początkowych).
- The system does not find the initial program or menu when you create profiles (Podczas tworzenia profili system nie odnalazł programu lub menu początkowego).

Do czasu załadowania bibliotek aplikacji nie da się przetestować opisów zadań i profili.

Należy skorzystać z Formularzy instalowania aplikacji, przygotowanych w sekcji ″Planowanie instalowania aplikacji.″

Aby załadować każdą aplikację, należy wykonać następujące zadania:

1. Tworzenie profilu właściciela.
2. Ładowanie aplikacji.

Wpisywanie się do systemu

- Aby utworzyć profile właścicieli:

  Profil Własny (wymagane uprawnienia *SECADM)

Menu MAIN (Główne)

- Aby załadować biblioteki aplikacji:

  Z dostawcą aplikacji należy sprawdzić, czy podczas ładowania aplikacji użytkownik powinien być wpisany jako szef ochrony, czy jako właściciel aplikacji.

Po wpisaniu się można utworzyć profil właściciela aplikacji.

Tworzenie profilu właściciela

Po wpisaniu się do systemu należy sprawdzić Planowanie instalowania aplikacji, aby ustalić, czy przed ładowaniem aplikacji należy utworzyć jakiekolwiek profile. Aby utworzyć profil:

1. Wpisz CRTUSRPRF (Tworzenie profilu użytkownika - Create User Profile) i naciśnij klawisz **F4** (Podpowiedź).
2. Na ekranie Tworzenie profilu użytkownika (Create User Profile) wypełnij pola zgodnie z instrukcjami programisty lub dostawcy aplikacji.
3. Naciśnij klawisz **F10** (Więcej pól) i przejdź do następnej strony, aby wyświetlić dodatkowe pola.

```
            Tworzenie profilu użytkownika
          (Create User Profile - CRTUSRPRF)
Wypełnij pola i naciśnij Enter

Profil użytkownika . . . . . >
Hasło użytkownika. . . . . .   *USRPRF
Ustawienie jako wygasłe hasła. .   *NO
Status . . . . . .   *ENABLED
Klasa użytkownika. . . . . .   *USER
Poziom asysty. . . . . .   *SYSVAL
Biblioteka bieżąca . . . . . .   *CRTDFT
Wywoływany program początkowy. .   *NONE
  Biblioteka . . . . . .
Menu początkowe. . . . . .   MAIN
  Biblioteka . . . . . .     *LIBL
Ograniczenie możliwości. . . . .   *NO
Tekst opisu. . . . . .   Właściciel xxxxxx
```

4. Sprawdź, czy w dole ekranu zostały wyświetlone jakieś komunikaty.

Uwaga: Proces tworzenia profili został szczegółowo omówiony w temacie Tworzenie profilu grupowego.

Po utworzeniu właściciela aplikacji można rozpocząć ładowanie aplikacji.

Ładowanie aplikacji

W celu załadowania bibliotek aplikacji należy wykonać instrukcje dostarczone przez dostawcę aplikacji. W sekcji ″Ustawianie praw własności i uprawnień publicznych″ znajdują się instrukcje dotyczące ustawiania praw własności i uprawnień publicznych dla aplikacji.

Po załadowaniu wszystkich aplikacji można skonfigurować grupy użytkowników.

Konfigurowanie grup użytkowników

Po wykonaniu czynności dotyczących ochrony podczas ładowania aplikacji można skonfigurować grupy użytkowników. Następnie można utworzyć biblioteki dla grup, opisy zadań oraz profile grupowe. W trakcie czytania tego tematu należy pracować z jedną grupą, a następnie wrócić do tego miejsca i powtórzyć te czynności dla pozostałych grup. Przykładowe ekrany zawierają informacje z Formularzy opisywania grup użytkowników dla działu sprzedaży i marketingu oraz magazynu przedsiębiorstwa JKL Toy Company.

W tym temacie należy korzystać z Formularzy opisywania grup użytkowników, przygotowanych w sekcji ″Planowanie grup użytkowników.″

Aby skonfigurować grupy użytkowników, należy wykonać następujące zadania:

1. Tworzenie biblioteki dla grupy użytkowników.
2. Tworzenie opisu zadania.
3. Tworzenie profilu grupowego.

Wpisywanie się do systemu

Profil Własny (wymagane uprawnienia *SECADM)

Menu MAIN (Główne)

Po wpisaniu się można utworzyć bibliotekę dla grupy użytkowników.

Tworzenie biblioteki dla grupy

Po wpisaniu się do systemu należy utworzyć bibliotekę dla grupy użytkowników. Jeśli grupa ma współużytkować bibliotekę dla obiektów, które tworzy, na przykład dla zapytań Query, bibliotekę należy utworzyć przed utworzeniem profilu grupowego:

1. Wpisz CRTLIB (Tworzenie biblioteki - Create Library) i naciśnij klawisz **F4** (Podpowiedź).
2. Wypełnij ekran. Nazwa biblioteki powinna być taka sama, jak nazwa profilu.
3. Naciśnij klawisz **F10** (Parametry dodatkowe).
4. Podaj uprawnienia publiczne do biblioteki oraz do nowych obiektów tworzonych w bibliotece.
5. Naciśnij klawisz **Enter**. Sprawdź komunikat potwierdzający.

```
                          Tworzenie biblioteki
                           (Create Library)

Wypełnij pola i naciśnij Enter

Biblioteka . . . . . .   DPTWH
Typ biblioteki . . . . . .   *PROD
Tekst opisu. . . . . .   Biblioteka magazynu

                          Parametry dodatkowe

Uprawnienie. . . . . .   *USE
ID puli pamięci dyskowej . . . . .   1
Uprawnienie do tworzenia . . . . .   *CHANGE
Kontrola tworzonego obiektu. . . .   *SYSVAL
```

Możliwy błąd	Rozwiązanie
Przed wpisaniem opisu biblioteki naciśnięto klawisz **Enter**.	Wpisz **CHGLIB** i naciśnij klawisz **F4** (Podpowiedź). Wpisz nazwę biblioteki i naciśnij klawisz **Enter**. Na ekranie Zmiana biblioteki (Change Library) podaj opis biblioteki.
Bibliotece nadano złą nazwę.	Skorzystaj z komendy Zmiana nazwy obiektu (Rename Object - RNMOBJ).

Po utworzeniu biblioteki dla grupy, można utworzyć opis zadania.

Tworzenie opisu zadania

Po utworzeniu biblioteki dla grupy, dla każdej grupy można utworzyć opis zadania.

Jeśli w systemie nie ma jeszcze bibliotek wymaganych dla początkowej listy bibliotek, podczas tworzenia opisu zadania pojawi się komunikat ostrzegawczy.

1. Wpisz **CRTJOBD** (Tworzenie opisu zadania - Create Job Description) i naciśnij klawisz **F4** (Podpowiedź).

2. Wypełnij następujące pola:

   Opis zadania:
   Taki sam, jak nazwa profilu grupowego.

   Nazwa biblioteki:
   QGPL

   Tekst: Opis grupy.
3. Naciśnij klawisz **F10** (Parametry dodatkowe).
4. Przejdź do następnej strony, do pola *Początkowa lista bibliotek*.

```
                      Tworzenie opisu zadania
                      (Create Job Description)

Wypełnij pola i naciśnij Enter

Opis zadania . . . . . .   DPTSM
  Biblioteka . . . . . .   QGPL
Kolejka zadań. . . . . .   QBATCH
  Biblioteka . . . . . .     *LIBL
Priorytet zadania (w JOBQ) . . . .   5
Priorytet wyjścia (w OUTQ) . . . .   5
Drukarka . . . . . . . . . . . .   *USRPRF
Kolejka wyjściowa. . . . . . . .   *USRPRF
  Biblioteka . . . . . .
Tekst opisu . . . . . .   Sprzedaż i marketing
```

5. Aby określić, że ma być podana lista wartości, nad parametrem *SYSVAL pola *Początkowa lista bibliotek* wpisz **+** (plus). Naciśnij klawisz **Enter**.

```
Kod rozliczeniowy . . . . . .   *USRPRF
  :
Sprawdzenie składni CL. . . . . .   *NOCHK
Początkowa lista bibliotek. . . . .   +
              + dla więcej
```

6. W polu *Początkowa lista bibliotek* wpisz nazwy bibliotek, które zostały zaznaczone (✓) na Formularzu opisywania grupy użytkowników:
   - W jednym wierszu wpisz jedną bibliotekę.
   - Podaj także biblioteki QGPL i QTEMP. Każde zadanie do przechowywania obiektów tymczasowych, wykorzystuje bibliotekę QTEMP. **Wszystkie początkowe listy bibliotek muszą zawierać bibliotekę QTEMP**. Dla większości aplikacji na początkowej liście bibliotek powinna być także biblioteka QGPL.
   - Na liście bibliotek nie trzeba podawać biblioteki bieżącej (domyślnej). System dodaje ją automatycznie podczas wpisywania się.
7. Naciśnij klawisz **Enter**. Sprawdź komunikaty. (Przejdź do następnej strony, aby zobaczyć wszystkie komunikaty.)

```
                           Określanie więcej wartości dla
                             (Specify More Values for)

Wypełnij pola i naciśnij Enter

Początkowa lista bibliotek. . . .    CUSTLIB
ITEMLIBCOPGMLIBICPGMLIB                                QGPL
                                     QTEMP
```

Możliwy błąd	Rozwiązanie
Zamiast klawisza **F10** naciśnięto klawisz **Enter**.	Aby umieścić poprawną bibliotekę na początkowej liście bibliotek, wpisz **CHGJOBD** (Zmiana opisu zadania - Change Job Description) i naciśnij klawisz **F4**.
Podczas tworzenia opisu zadania pojawiają się komunikaty o błędach.	Najczęściej wyświetlany jest komunikat o błędzie informujący, że użytkownik próbuje dodać bibliotekę, której nie ma w systemie. Jest to komunikat ostrzegawczy. Opis zadania nadal jest tworzony z biblioteką na początkowej liście bibliotek. Jednak jeśli biblioteki nie ma w sysytemie, nie można wpisać się za pomocą profilu z opisem zadania. Jeśli biblioteka jest w systemie, prawdopodobnie nieprawidłowo wpisano jej nazwę. Sprawdź nazwę biblioteki i spróbuj ponownie.

Po utworzeniu opisu zadania można utworzyć profil grupowy.

Tworzenie profilu grupowego

Po utworzeniu opisu zadania można utworzyć profil grupowy. Aby to zrobić, należy wykorzystać informacje z części 2 Formularza opisywania grupy użytkowników.

1. Użyj komendy Praca z profilami użytkowników (Work with User Profiles). Wpisz WRKUSRPRF *ALL. Początkowo na ekranie wyświetlana jest lista profili dostarczanych przez firmę IBM.

   Uwaga: Jeśli zostanie wyświetlony ekran Praca z rejestrowaniem użytkowników (Work with User Enrollment), naciśnij klawisz **F21**, aby zmienić na intermediate assistance level.

2. Aby utworzyć nowy profil, w kolumnie *Opcja* wpisz **1**, a w kolumnie *Profil użytkownika* nazwę profilu. Naciśnij klawisz **Enter**.

```
                     Praca z profilami użytkowników
                       (Work with User Profiles)

Wpisz opcje i naciśnij klawisz Enter.
  1=Utwórz  2=Zmień   3=Kopiuj   4=Usuń   5=Wyświetl
  12=Praca z obiekt. wg właścicieli

     Profil
Opc  użytkownika Tekst
1    DPTSM
     QDOC        Profil użytkownika
     QSECOFR     Profil użytkownika szefa ochrony
```

3. W odpowiednich polach wpisz informacje z Formularza opisywania grupy użytkowników.
4. Aby pominąć pola, w których mają pozostać wartości domyślne, użyj klawisza **Tab**.
5. Naciśnij klawisz **F10** (Parametry dodatkowe).
6. Przejdź do następnej strony.

```
            Tworzenie profilu użytkownika
          (Create User Profile - CRTUSRPRF)
Wypełnij pola i naciśnij Enter

Profil użytkownika . . . . . > DPTSM
Hasło użytkownika. . . . . .   *none
Ustawienie jako wygasłe hasła. .   *NO
Status . . . . . .   *ENABLED
Klasa użytkownika. . . . . .   *USER
Poziom asysty. . . . . .   *SYSVAL
Biblioteka bieżąca . . . . . .   *CRTDFT
Wywoływany program początkowy. .   cpsetup
  Biblioteka . . . . . .   cppgmlib
Menu początkowe. . . . . .   cpmain
  Biblioteka . . . . . .   cppgmlib
Ograniczenie możliwości. . . . .   *yes
Tekst opisu. . . . . .   Sales and Marke
```

7. Na dodatkowych stronach wypełnij pozostałe pola, podając informacje z Formularza opisywania grupy użytkowników, a następnie naciśnij klawisz **Enter**.

```
                     Tworzenie profilu użytkownika
                         (Create User Profile)

                          Parametry dodatkowe

Uprawnienia specjalne. . . . . .   *USRCLS

   :
Opis zadania . . . . . .   DPTSM
  Biblioteka . . . . . .   QGPL
```

```
                     Tworzenie profilu użytkownika
                         (Create User Profile)

Uprawnienie grupowe. . . . . .   *NONE

   :
Drukarka. . . . . .   PRT03
```

8. Sprawdź komunikaty.

Pamiętaj

Profil grupowy jest po prostu szczególnym rodzajem profilu użytkownika. Wiele komunikatów i ekranów odnosi się do profili grupowych, tak jak do użytkowników lub do profili użytkowników. System wie o tym, że profil grupowy został utworzony, tylko jeśli do profilu zostanie dodany użytkownik lub przypisany numer identyfikacyjny grupy (gid).

Możliwy błąd	Rozwiązanie
Przed wpisaniem wszystkich wartości dla profilu grupowego naciśnięto klawisz **Enter**.	Naciśnij klawisz **F5** (Odśwież), aby utworzony profil dodać do ekranu Praca z profilami użytkowników (Work with User Profiles). Aby poprawić profil, skorzystaj z opcji **2** (Zmień).

Możliwy błąd	Rozwiązanie
Utworzono profil z błędną nazwą.	Nie można zmienić nazwy profilu. Użyj opcji kopiowania (**3**), aby utworzyć nowy profil z prawidłową nazwą. Następnie usuń (opcja **4**) profil z błędną nazwą.
Nie które pola Formularza opisywania grupy użytkowników nie pojawiają się na ekranie.	Upewnij się, że używany jest intermediate assistance level. Wersja podstawowy poziom asysty ekranu Tworzenie profilu użytkownika (Create User Profile) to ekran Dodawanie Użytkownika (Add a User). Aby zmienić poziom asysty, naciśnij klawisz **F12** (Anuluj) i wróć do ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment). Aby zmienić poziom asysty, użyj klawisza **F21**. Więcej informacji na ten temat zawiera sekcja ″Wybieranie odpowiedniego poziomu asysty.″
Przypadkowo skasowano niektóre informacje domyślne na ekranie Tworzenie profilu użytkownika (Create User Profile).	Jeśli pole będzie puste, podczas tworzenia profilu użytkownika system użyje wartości domyślnych. Jeśli wartości domyślne mają być widoczne, użyj klawisza **F5** (Odśwież), aby odtworzyć cały ekran. Ponownie wpisz swoje informacje.

Listing wyników

Za pomocą komendy Wyświetlenie uprawnionych użytkowników (Display Authorized Users - DSPAUTUSR) można wyświetlić listę nazw i opisów wszystkich profili w systemie. Należy wpisać DSPAUTUSR OUTPUT(*PRINT). Następnie należy upewnić się, że wszystkie profile grupowe mają hasło *NONE.

Przed skonfigurowaniem pojedynczych użytkowników, należy wykonać następujące czynności:

- Tworzenie opisu zadania dla każdej grupy użytkowników.
- Opcjonalnie, tworzenie biblioteki dla każdej grupy.
- Tworzenie profilu grupowego dla każdej grupy użytkowników.

Konfigurowanie pojedynczych użytkowników

Konfigurowanie grup użytkowników było ostatnią czynnością dotyczącą tworzenia profili grupowych. Teraz utworzone zostaną pojedyncze profile dla członków tych grup.

W trakcie czytania tego tematu należy pracować z członkami jednej grupy, a następnie wrócić do tego miejsca i powtórzyć wszystkie czynności dla pozostałych grup. Przykładowe ekrany zawierająużytkowników z formularzy Formularz pojedynczego profilu użytkownika, które Sharon Jones przygotowała dla działu sprzedaży i marketingu oraz magazynu w przedsiębiorstwie JKL Toy Company. Kopie tych formularzy można znaleźć w sekcji ″Planowanie pojedynczych profili użytkowników.″

W tym temacie należy korzystać z Formularzy pojedynczych profili użytkowników, które zostały przygotowane w sekcji ″Planowanie pojedynczych profili użytkowników.″

Aby utworzyć pojedyncze profile dla członków grup, należy wykonać następujące czynności:

1. Tworzenie biblioteki osobistej. (opcjonalne)
2. Kopiowanie profilu grupowego.
3. Ustawianie utraty ważności hasła.
4. Tworzenie dodatkowych użytkowników. (opcjonalne)

   Uwaga: Czynności Tworzenie biblioteki osobistej i Tworzenie dodatkowych użytkowników należy powtarzać, aż zostaną utworzone profile dla wszystkich członków grupy.
5. Jeśli to konieczne, należy zmienić informacje o użytkowniku.
6. Wyświetlanie wyników.

Wpisywanie się do systemu

Profil Własny (wymagane uprawnienia *SECADM)

Menu SETUP (Konfigurowanie)

Tworzenie biblioteki osobistej

Aby rozpocząć konfigurowanie pojedynczych użytkowników, dla każdego członka grupy należy utworzyć bibliotekę osobistą, w której będą przechowywane jego obiekty, na przykład zapytania Query. Biblioteki osobiste należy utworzyć przed tworzeniem pojedynczych profili użytkowników.

1. Wpisz **CRTLIB** i naciśnij klawisz **F4** (Podpowiedź).
2. Nadaj bibliotece taką samą nazwę, jaką ma profil użytkownika.
3. Naciśnij klawisz **F10** (Parametry dodatkowe).
4. Podaj uprawnienia publiczne do biblioteki oraz do nowych obiektów tworzonych w bibliotece.
5. Naciśnij klawisz **Enter**. Sprawdź komunikat potwierdzający.

```
                          Tworzenie biblioteki
                           (Create Library)

Wypełnij pola i naciśnij Enter

Biblioteka . . . . . .   DPTSM
Typ biblioteki . . . . . .   *PROD
Tekst opisu. . . . . .   Biblioteka magazynu

                          Parametry dodatkowe

Uprawnienie. . . . . .   *EXCLUDE
ID puli pamięci dyskowej . . . .   1
Uprawnienie do tworzenia . . . .   *CHANGE
Kontrola tworzonego obiektu. . .   *SYSVAL
```

Po utworzeniu biblioteki osobistej można skopiować profil grupowy i można utworzyć pojedynczy profil.

Kopiowanie profilu grupowego

Profil grupowy spełnia dwie role:

1. system używa go do określenia, czy członek grupy ma uprawnienia do używania obiektu,
2. można go użyć jako wzorca do tworzenia profili użytkowników dla pojedynczych członków grupy.

Konfigurowanie grup użytkowników było ostatnią czynnością tworzenia profili grupowych. Teraz można skopiować profil grupowy i utworzyć profil pojedynczego użytkownika, który również można skopiować i na jego podstawie utworzyć profile pozostałych członków grupy.

1. Z menu menu SETUP wybierz opcję Praca z rejestrowaniem użytkowników (Work with User Enrollment).

   Uwaga: Jeśli zostanie wyświetlone menu Praca z profilami użytkowników (Work with User Profiles), naciśnij klawisz **F21** (Wybór poziomu asysty), aby zmienić podstawowy poziom asysty.
2. W kolumnie *Opcja* obok grupy użytkowników wpisz **3** (Kopiuj). Pojawi się ekran Kopiowanie użytkowników (Copy User). (Jeśli grupy, która ma być skopiowana, nie ma na ekranie, przejdź do następnej strony, aż ją odnajdziesz.) System pozostawia puste pole nazwy użytkownika, a resztę wypełnia danymi z kopiowanego profilu grupowego.

```
            Praca z rejestrowaniem użytkowników
               (Work with User Enrollment)

 Wpisz opcje i naciśnij klawisz Enter.
  1=Dodaj   2=Zmień   3=Kopiuj   4=Usuń   5=Wyświetl

Opc     Użytkownik         Opis

        DPTSM          Dział sprzedaży i marketingu
3       DPTWH          Magazyn
```

3. Wpisz nazwę i opis tworzonego profilu użytkownika.
4. Hasło pozostaw puste. System automatycznie ustawi hasło, które będzie takie samo jak nazwa profilu użytkownika.
5. W polu *Grupa użytkowników* podaj nazwę profilu grupowego.
6. Sprawdź Formularz pojedynczego profilu użytkownika, aby przekonać się, czy dany użytkownik ma inne wartości niż grupa. Podaj te wartości.
7. Przejdź do następnej strony.

```
                      Kopiowanie użytkowników
                           (Copy User)

Kopiowanie użytkownika. :   DPTWH

Wpisz opcje i naciśnij klawisz Enter.

Użytkownik. . . . . .   WILLISR
Opis użytkownika  . . .   Willis, Rose
Hasło. .  . . . . . .
Typ użytkownika . . . . .   *SYSOPR
Grupa użytkowników. . . .   DPTWH

Ogranicz. użycia w.komend   N

Biblioteka domyślna . . .   DPTWH
Drukarka domyślna . . . .   PRT04
Program początkowy. . . .   *NONE
Biblioteka. . . . . .

Menu początkowe . . . . .   ICMAIN
  Biblioteka. . . . . .      ICPGMLIB
```

8. Wprowadź niezbędne zmiany na następnej stronie ekranu i naciśnij klawisz **Enter**.
9. Sprawdź komunikaty potwierdzenia pojawiające się u dołu ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment).

```
                      Kopiowanie użytkowników
                           (Copy User)

Kopiowanie użytkownika. :   DPTWH

Wpisz opcje i naciśnij klawisz Enter.

program klawisza ATTN . .   *SYSVAL
Biblioteka. . . . . .
```

Możliwy błąd	Rozwiązanie
Zamiast ekranu Kopiowanie użytkowników (Copy User) widać ekran Tworzenie profilu użytkownika (Create User Profile).	Aby powrócić do ekranu Praca z profilami użytkowników (Work with User profile), naciśnij klawisz **F12** (Anuluj). Naciśnij klawisz **F21**, aby zmienić na podstawowy poziom asysty. Jeszcze raz rozpocznij operację kopiowania.
Wybrana nazwa profilu użytkownika nie zmieści się w podpowiedzi.	Wprawdzie nazwa profilu użytkownika może mieć do 10 znaków, ekrany Kopiowanie użytkowników (Copy User) oraz Dodawanie użytkowników (Add User) nie obsługują więcej niż 8 znaków. Należy wybrać krótszą nazwę użytkownika lub skorzystać z intermediate assistance level.

Testowanie profilu użytkownika

Po utworzeniu w grupie pierwszego pojedynczego profilu, należy go przetestować wpisując się do systemu. Należy sprawdzić, czy pojawia się poprawne pierwsze menu oraz czy program wpisywania się został uruchomiony.

Jeśli nie da się wpisać za pomocą tego profilu, system prawdopodobnie nie mógł odnaleźć niektórych elementów określonych w profilu. Może to być program wpisywania się, opis zadania lub jedna z bibliotek z początkowej listy bibliotek. Aby odszukać protokół zadania, który został zapisany podczas próby wpisywania się, należy skorzystać z ekranu Praca z wydrukami (Work with Printer Output). Protokół zadania zawiera informacje na temat błędów, które wystąpiły.

Informacje na temat testowania i diagnozowania problemów związanych ze zmianami ochrony, zawiera sekcja ″Testowanie ochrony.″

Po przetestowaniu profilu użytkownika można ustawić hasło jako wygasłe.

Ustawianie hasła jako wygasłe

Pojedyncze profile należy tak skonfigurować, aby wymagały zmiany hasła po pierwszym wpisaniu się. Pole *Ustawienie hasła jako wygasłe* nie pojawia się w wersji podstawowy poziom asysty ekranu Kopiowanie użytkowników (Copy User). Należy zmienić je oddzielnie, po utworzeniu profilu za pomocą funkcji kopiowania. Aby zmienić pole *Ustawienie hasła jako wygasłe*, należy wpisać CHGUSRPRF *nazwa_profilu* PWDEXP(*YES).

Uwaga: Jeśli profil użytkownika ma być testowany przez wpisanie się za jego pomocą, test należy wykonać *przed* ustawieniem hasła jako wygasłe.

Możliwy błąd	Rozwiązanie
Podczas testowania hasła trzeba było zmienić hasło.	Wpisz **CHGUSRPRF** *nazwa_profilu* i naciśnij klawisz **F4** (Podpowiedź). Z powrotem ustaw hasło na nazwę profilu. (W polu hasła wpisz nazwę profilu użytkownika.) W polu *Ustawienie hasła jako wygasłe* wpisz ***YES**. Aby to zrobić, potrzebny jest intermediate assistance level.

Po utworzeniu pierwszego pojedynczego profilu użytkownika można utworzyć dodatkowych użytkowników.

Tworzenie dodatkowych użytkowników

Po skopiowaniu profilu grupowego w celu utworzenia pierwszego pojedynczego profilu, można utworzyć dodatkowych użytkowników. Aby utworzyć dodatkowych członków grupy, należy skopiować profil pierwszego pojedynczego użytkownika. Podczas tworzenia za pomocą kopiowania należy uważnie obserwować każdy pojedynczy profil. Należy sprawdzić Formularz pojedynczego profilu użytkownika i upewnić się, że zmienione zostały wszystkie pola, które są unikalne dla nowego profilu użytkownika.

1. Na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment) obok profilu użytkownika, który ma być skopiowany, wpisz **3** (Kopiowanie).
2. Na ekranie Kopiowanie użytkowników (Copy User) wpisz nazwę i opis profilu.

3. Wpisz informacje w polach, które są unikalne dla nowego użytkownika.

```
            Praca z rejestrowaniem użytkowników
               (Work with User Enrollment)

 Wpisz opcje i naciśnij klawisz Enter.
  1=Dodaj   2=Zmień   3=Kopiuj   4=Usuń   5=Wyświetl

Opc     Użytkownik         Opis

        DPTSM          Dział sprzedaży i marketingu
        DPTWH          Magazyn
3       WILLISR        Willis, Rose
```

Możliwy błąd	Rozwiązanie
Profil, który ma być skopiowany, nie pojawia się na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment).	Naciśnij klawisz **F5** (Odśwież). Przejdź do poprzedniej strony i do następnej. Lista jest ułożona alfabetycznie, według nazw profili.

Jeśli trzeba zmienić informacje na temat użytkownika, należy zapoznać się z sekcją Zmienianie informacji o użytkowniku.

Zmienianie informacji o użytkowniku

W przypadku niektórych użytkowników konieczne może być ustawienie wartości, które nie pojawiają się na ekranie Kopiowanie użytkowników (Copy User). Na przykład niektórzy użytkownicy mogą należeć do więcej niż jednego profilu grupowego. Po utworzeniu profilu użytkownika za pomocą metody kopiowania, można go zmienić.

1. Na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment) naciśnij klawisz **F21**, aby zmienić na intermediate assistance level.
2. Na ekranie Praca z profilami użytkowników (Work with User Profiles), w kolumnie *Opcja* obok profilu, który ma być zmieniany, wpisz **2** (Zmiana). Naciśnij klawisz **Enter**.

```
                     Praca z profilami użytkowników
                       (Work with User Profiles)

Wpisz opcje i naciśnij klawisz Enter.
  1=Utwórz  2=Zmień   3=Kopiuj   4=Usuń   5=Wyświetl
  12=Praca z obiekt. wg właścicieli

     Profil
Opc  użytkownika Tekst
2    AMESJ       Ames, Janice
     DPTSM       Dział sprzedaży i marketingu
     QDOC        Profil użytkownika
     QSECOFR     Profil użytkownika szefa ochrony
     WAGNERR     Wagner, Ray
     WILLISR     Willis, Rose
```

3. Na ekranie Zmiana profilu użytkownika (Change User Profile) naciśnij klawisz **F10** (Parametry dodatkowe).
4. Przejdź do następnej strony, aż znajdziesz pola, które mają być zmienione. Na przykład jeśli użytkownik ma być członkiem dodatkowego profilu grupowego, należy przejść do następnej strony i odszukać pola *Grupy dodatkowe*.
5. Wpisz odpowiednie wartości i naciśnij klawisz **Enter**. Zostaną wyświetlone komunikaty potwierdzające i ekran Praca z profilami użytkowników (Work with User Profiles).

```
                        Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF)

Wypełnij pola i naciśnij Enter

Maks. dopuszczalna pamięć. . . .   *NOMAX
Najwyższy priorytet w harmon.. .   3
Opis zadania. .  . . . . . .  .   DPTWH
  Biblioteka . . . . . . . . .      QGPL
Profil grupowy . . . . . . . .   DPTWH
Właściciel . . . . . . . . . .   *GRPPRF
Uprawnienie grupowe. . . . . .   *USEE
Typ uprawnień grupowych. . . .   *PGP
Grupy dodatkowe. . . . . . . .   DPTIC
               + dla więcej
```

Po zmianie informacji o użytkowniku można wyświetlić wyniki, aby sprawdzić profile.

Wyświetlanie profili użytkowników

Jest kilka metod wyświetlania utworzonych profili.

Wyświetlanie jednego profilu
Na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment) lub Praca z profilami użytkowników (Work with User Profiles) należy użyć opcji **5** (Wyświetlenie).

Listing jednego profilu
Należy użyć komendy Wyświetlenie profilu użytkownika (Display User Profile): DSPUSRPRF *nazwa_profilu* DETAIL(*BASIC) OUTPUT(*PRINT).

Wyświetlanie członków grupy
Należy wpisać DSPUSRPRF *nazwa_profilu_grupowego* *GRPMBR. Aby wydrukować listę, można użyć komendy OUTPUT(*PRINT).

Listing wszystkich profili
Aby wyświetlić listę i opisy wszystkich profili, posortowanych według grup, należy użyć komendy Wyświetlenie uprawnionych użytkowników (Display Authorized Users): DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT).

Przed ustawieniem praw własności i uprawnień publicznych, należy upewnić się, że wykonane zostały następujące czynności:

- Utworzono wszystkie pojedyncze profile użytkowników.
- Ustawiono hasło jako wygasłe.
- Wydrukowano listę wszystkich profili posortowanych według grup i schowano ją razem z Formularzami opisywania grup użytkowników. Po dodaniu nowych użytkowników listę należy wydrukować ponownie.

Konfigurowanie ochrony zasobów

W tym temacie opisano sposób ustawiania praw własności i uprawnień publicznych dla obiektów i uprawnień dla aplikacji. Opisano także skonfigurowanie ochrony zasobów dla stacji roboczych i drukarek. W trakcie czytania tego tematu należy pracować z jedną biblioteką, a następnie wrócić do tego miejsca i powtórzyć wszystkie czynności dla pozostałych bibliotek. Po skonfigurowaniu ochrony zasobów dla jednej aplikacji, wszystkie czynności należy powtórzyć dla innych aplikacji.

Przedstawione procedury należy wykorzystywać zawsze podczas instalowania w systemie nowej aplikacji lub konfigurowania ochrony zasobów istniejącej aplikacji.

Przykładowe ekrany zawierają dane z Formularzy list autoryzacji, Formularzy opisywania biblioteki oraz Formularzy ochrony kolejki wyjściowej i stacji roboczej dla przedsiębiorstwa JKL Toy Company. Przykłady tych formularzy można znaleźć w sekcji ″Ustawianie praw własności i uprawnień publicznych.″

Które formularze są potrzebne?

- Formularze instalowania aplikacji przygotowane w sekcji ″Planowanie instalowania aplikacji.″
- Formularze list autoryzacji przygotowane w sekcji ″Grupowanie obiektów.″
- Formularze opisywania biblioteki przygotowane w sekcji ″Określanie praw własności do bibliotek i obiektów.″
- Formularz ochrony kolejki wyjściowej i stacji roboczej przygotowany w sekcjach ″Zabezpieczanie wydruków″ i ″Zabezpieczanie stacji roboczych.″
- Formularz odpowiedzialności w systemie przygotowany w sekcji ″Planowanie ogólnej strategii ochrony.″

Ochronę zasobów można skonfigurować na kilka sposobów. Kolejność czynności opisanych w tym temacie jest zgodna z kolejnością informacji podanych w Formularzach instalowania aplikacji, Formularzach list autoryzacji i Formularzu opisywania biblioteki:

1. Konfigurowanie praw własności oraz uprawnień publicznych.
2. Tworzenie list autoryzacji.
3. Zabezpieczanie obiektów za pomocą listy autoryzacji.
4. Dodawanie użytkowników do list autoryzacji.
5. Ustawianie uprawnień szczegółowych.
6. Zabezpieczanie zbiorów wydruków.
7. Zabezpieczanie stacji roboczych.
8. Ograniczanie dostępu do kolejki komunikatów operatora systemu.

Ustawianie praw własności oraz uprawnień publicznych

W tym temacie ustawione zostaną prawa własności i uprawnienia publiczne do bibliotek aplikacji, bibliotek dla grup i bibliotek osobistych. W trakcie czytania tego tematu należy pracować z jedną aplikacją, a następnie wrócić do tego miejsca i powtórzyć wszystkie czynności dla pozostałych aplikacji. Przykładowe ekrany prezentują Formularze instalowania aplikacji, które zostały przygotowane przez Sharon Jones w sekcji ″Planowanie instalowania aplikacji″, dla aplikacji Zamówienia klientów.

Przedstawione w tym temacie procedury należy wykorzystywać podczas instalowania w systemie nowych aplikacji lub konfigurowania ochrony dla istniejącej aplikacji.

Należy skorzystać z Formularzy instalowania aplikacji, przygotowanych w sekcji ″Planowanie instalowania aplikacji.″

Aby ustawić prawa własności i uprawnienia publiczne, należy wykonać następujące czynności:

1. Tworzenie profilu właściciela.
2. Zmienianie praw własności do biblioteki.
3. Ustawianie praw własności dla obiektów aplikacji.
4. Ustawianie dostępu publicznego do biblioteki.
5. Ustawianie uprawnień publicznych dla wszystkich obiektów w bibliotece.
6. Ustawianie uprawnień publicznych dla nowych obiektów.
7. Praca z bibliotekami dla grup i osobistymi.

Wpisywanie się do systemu

Profil Własny (wymagane uprawnienia *ALLOBJ)

Menu MAIN (Główne)

Tworzenie profilu właściciela

Jeśli profil właściciela jeszcze nie istnieje, należy wykonać następujące czynności:

- Utwórz profil za pomocą komendy Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF). Ustaw hasło na wartość *NONE.

Jeśli profil właściciela już istnieje, należy wykonać następujące czynności:

- Za pomocą komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF) ustaw hasło na wartość *NONE.

Po utworzeniu profilu właściciela można zmienić prawa własności do biblioteki.

Zmienianie prawa własności do biblioteki

Przedstawiona w tej sekcji czynność zmienia prawa własności do biblioteki, a nie do obiektów w bibliotece.

Uwaga: Przed zmianą praw własności do jakichkolwiek obiektów aplikacji należy skonsultować się z dostawcą aplikacji. Niektóre aplikacje korzystają z funkcji, które wykorzystująprawa własności do obiektu.

1. Wpisz CHGOBJOWN (Zmiana właściciela obiektu - Change Object Owner) i naciśnij klawisz **F4** (Podpowiedź).
2. Podaj nazwę biblioteki, rodzaj obiektu (*LIB) i nowego właściciela.
3. Sprawdź komunikaty potwierdzenia.

```
                Zmiana właściciela obiektu
             (Change Object Owner - CHGOBJOWN)
Wypełnij pola i naciśnij Enter

Obiekt . . . . . . . . . . . . . > COPGMLIB
  Biblioteka . . . . . . . . . . >   *LIBL       Nazwa,
Typ obiektu  . . . . . . . . . .> *LIB
Nowy właściciel. . . . . . . . .   COWNER
Upraw.bieżącego właściciela. . .   *REVOKE
```

Możliwy błąd	Rozwiązanie
Otrzymano komunikaty o błędach.	Najczęściej komunikat informuje o tym, że nie można znaleźć biblioteki lub profilu nowego właściciela. Sprawdź, czy nie popełniono błędu podczas wpisywania, i spróbuj ponownie.

Po zmianie praw własności do biblioteki można ustawić prawa własności do obiektów aplikacji.

Ustawianie praw własności do obiektów aplikacji

Zmiana praw własności do obiektów aplikacji to ciężkie zadanie, ponieważ każdy obiekt trzeba zmieniać pojedynczo. Jeśli to możliwe, należy poprosić programistę lub dostawcę aplikacji o ustanowienie praw własności.

Listing obiektów w bibliotece

Przed zmianą praw własności za pomocą komendy Wyświetlenie biblioteki (Display Library) należy wydrukować listę wszystkich obiektów w bibliotece. Można jej użyć jako listy kontrolnej. W tym celu należy wpisać DSPLIB *nazwa_biblioteki* *PRINT.

Wybieranie najlepszej metody

Aby zmienić prawa własności do obiektów w bibliotekach aplikacji, należy użyć jednej z metod:

Tabela 61. Metody zmiany praw własności do obiektu

Metoda	Co robi	Kiedy używać
Komenda Praca z obiektami wg właścicieli (Work with Objects by Owner)	Wyświetla ekran z listą wszystkich obiektów należących do profilu. Do zmiany właściciela obiektu używana jest opcja z tego ekranu.	Ta metoda jest łatwiejsza w użyciu. Jednak jeśli właścicielami obiektów są profile QPGMR lub QSECOFR, firma IBM nie zaleca tej metody. Te profile są właścicielami wielu obiektów i wyświetlana lista może być bardzo duża.

Tabela 61. Metody zmiany praw własności do obiektu (kontynuacja)

Metoda	Co robi	Kiedy używać
Komenda Zmiana prawa własności do obiektu (Change Object Ownership)	Wymaga wywołania komendy dla każdego obiektu oddzielnie. Jednak w celu powtórzenia poprzedniej komendy i zredukowania konieczności pisania, można użyć opcji *Retrieve* (Wczytanie) (klawisz **F9**).	Ta metoda jest szybsza w przypadku, gdy właścicielami obiektów są profile QPGMR lub QSECOFR.

Korzystanie z komendy Praca z obiektami wg właścicieli (Work with objects by Owner - WRKOBJOWN): Jest to metoda zmiany praw własności dla obiektów w bibliotece, w przypadku gdy profile dostarczane przez firmę IBM, takie jak QPGMR lub QSECOFR, *nie* są właścicielami obiektów:

1. Wpisz WRKOBJOWN *nawa_profilu_właściciela*. Na ekranie pojawi się lista wszystkich obiektów, do których prawa ma ten profil użytkownika.
2. Obok każdego obiektu w bibliotece, z którą pracujesz, wpisz **9** (Zmiana właściciela).
3. W wierszu *Parametry lub komenda* u dołu ekranu, wpisz NEWOWN(*nazwa_profilu_właściciela*) i naciśnij klawisz **Enter**.
4. System zmieni właściciela dla każdego wskazanego obiektu na nowego, który został wpisany u dołu. U dołu ekranu pojawią się także komunikaty potwierdzające. Obiekty nie będą wyświetlane na ekranie, ponieważ profil nie jest już ich właściecielem.
5. Powtarzaj kroki 2 i 4, aż zmienisz prawa własności wszystkich obiektów w bibliotece.

```
           Praca z obiektami wg właścicieli
            (Work with Objects by Owner)

Profil użytkownika . . . . . :   OLDOWNER

Wpisz opcje i naciśnij klawisz Enter.
  2=Edytuj uprawnienie   4=Usuń   5=Wyświetl
  8=Wyświetl opis  9=Zmiana właściciela

Opc  Obiekt        Biblioteka     Typ      Atrybut
     COPGMMSG      COPGMLIB      *MSGQ
9    CUSTMAS       CUSTLIB       *FILE
9    CUSTMSGQ      CUSTLIB       *MSGQ
     ITEMMSGQ      ITEMLIB       *MSGQ


   ⋮

Parametry lub komenda
===> NEWOWN(COWNER)
F3=Wyjście   F4=Podpowiedź   F5=Odśwież  F9=Poprzednie komendy
F18=Koniec
```

Możliwy błąd	Rozwiązanie
Zostanie wyświetlony ekran Zmiana właściciela obiektu (Change Object Owner).	Ten ekran widać w przypadku, gdy podano opcję **9** (Zmiana właściciela) i u dołu ekranu Praca z obiektami wg właścicieli (Work with Objects by Owner) nie wpisano żadnych parametrów. Pojawia się on także po nieprawidłowym wpisaniu parametrów. Aby powrócić do ekranu Praca z obiektami wg właścicieli (Work with Objects by Owner), naciśnij klawisz **F12** (Anuluj). Spróbuj ponownie. Upewnij się, że parametry wpisywane są tak, jak w przykładzie.

Aby zmienić prawa własności dla obiektów, których właścicielami są profile QPGMR lub QSECOFR, można użyć komendy zmiany właściciela obiektu.

Używanie komendy Zmiana właściciela obiektu: Jest to metoda zmiany właściciela obiektów w bibliotece, stosowana w przypadku gdy profil QPGMR lub QSECOFR *mają* prawa własności dla obiektów.

1. Wpisz CHGOBJOWN i naciśnij klawisz **F4** (Podpowiedź).
2. Na ekranie podaj informacje dla pierwszego obiektu na liście i naciśnij klawisz **Enter**.

```
               Zmiana właściciela obiektu
            (Change Object Owner - CHGOBJOWN)
Wypełnij pola i naciśnij Enter

Obiekt . . . . . . . . . . . . . > CUSTMAS
  Biblioteka . . . . . . . . . . >   CUSTLIB
Typ obiektu  . . . . . . . . . . > *FILE
Nowy właściciel. . . . . . . . .   COWNER
Upraw.bieżącego właściciela. . .   *REVOKE
```

3. Pojawi się komunikat potwierdzający, że prawo własności do obiektu zostało zmienione. Sprawdź elementy listy.
4. Naciśnij klawisz **F9** (Wczytanie), aby wczytać wcześniej wpisaną komendę.
5. Naciśnij klawisz **F4** (Podpowiedź). Na ekranie Zmiana właściciela obiektu (Change Object Owner) podaj informacje dla następnego obiektu w bibliotece i naciśnij klawisz **Enter**.
6. Powtórz krok czwarty i piąty dla pozostałych obiektów.

Sprawdzanie

Aby upewnić się, że prawa własności do wszystkich obiektów w bibliotece zostały zmienione, należy użyć komendy Praca z obiektami wg właścicieli (Work with Objects by Owner). W tym celu należy wpisać WRKOBJOWN *profil_nowego_właściciela*. Następnie należy porównać ekran ze swoją listą obiektów w bibliotece.

Po zmianie praw własności do obiektów w bibliotece, można ustawić dostęp publiczny do biblioteki.

Ustawianie dostępu publicznego do biblioteki

Po ustawieniu praw własności dla obiektów aplikacji, za pomocą komendy Edycja uprawnień dla obiektu (Edit Object Authority - EDTOBJAUT) można zmienić uprawnienia publiczne do biblioteki:

1. Wpisz EDTOBJAUT *nazwa_biblioteki* *LIB.
2. Przesuń kursor na wiersz z wartością **PUBLIC*.
3. Wpisz uprawnienia publiczne, które mają mieć użytkownicy, i naciśnij klawisz **Enter**.

```
                         Edycja uprawnień dla obiektu
                           (Edit Object Authority)

Obiekt . . . . . . . :   CUSTLIB        Właściciel . . . . . :   COWNER
  Biblioteka . . . . :     QSYS         Grupa podstawowa . . :   *NONE
Typ obiektu  . . . . :   *LIB

Wprowadź zmiany w bieżących uprawnieniach i naciśnij Enter.

  Obiekt chroniony przez listę autoryzacji  . . . . . . . . . .   *NONE

                       Uprawnienie
Użytkownik  Grupa      do obiektu
COWNER                 *ALL
*PUBLIC                *CHANGE
```

4. Na ekranie zostaną wyświetlone nowe uprawnienia.

Teraz można ustawić uprawnienia publiczne do wszystkich obiektów w bibliotece.

Ustawianie uprawnień publicznych do wszystkich obiektów w bibliotece.

Aby usunąć aktualne uprawnienia publiczne dla obiektów biblioteki, należy użyć komendy Odwołanie uprawnień dla obiektu (Revoke Object Authority - RVKOBJAUT). Aby ustawić uprawnienia publiczne dla wszystkich obiektów w bibliotece, należy użyć komendy Nadanie uprawnień dla obiektu (Grant Object Authority - GRTOBJAUT):

1. Wpisz RVKOBJAUT i naciśnij klawisz **F4** (Podpowiedź).
2. Wypełnij ekran tak, jak to pokazano poniżej, zamieniając nazwę biblioteki aplikacji, i naciśnij klawisz **Enter**.

```
              Odwołanie uprawnień dla obiektu
            (Revoke Object Authority - RVKOBJAUT)

Wypełnij pola i naciśnij Enter

Obiekt . . . . . . . . . . . . .   *all
  Biblioteka . . . . . . . . . .     custlib
Typ obiektu  . . . . . . . . . .   *all
Użytkownicy. . . . . . . . . . .   *public
              + dla więcej
Uprawnienie. . . . . . . . . . .   *all
```

Uwaga: Jeśli w bibliotece znajduje się duża liczba obiektów, przetwarzanie żądania może zająć kilka minut.

3. W tym celu należy wpisać GRTOBJAUT i nacisnąć klawisz **F4** (Podpowiedź).
4. Wypełnij ekran, tak jak to pokazano poniżej, zamieniając nazwę biblioteki aplikacji i podając żądane uprawnienia, i naciśnij klawisz **Enter**.

```
                Nadanie uprawnień dla obiektu
              (Grant Object Authority - GRTOBJAUT)
Wypełnij pola i naciśnij Enter

Obiekt . . . . . . . . . . . . .   *all
  Biblioteka . . . . . . . . . .     custlib
Typ obiektu  . . . . . . . . . .   *all
Użytkownicy. . . . . . . . . . .   *public
              + dla więcej
Uprawnienie. . . . . . . . . . .   *use
```

Uwaga: Jeśli w bibliotece znajduje się duża liczba obiektów, przetwarzanie żądania może zająć kilka minut.

Po zakończeniu ustawiania uprawnień publicznych dla wszystkich obiektów w bibliotece można skorzystać z protokołu zadania, aby sprawdzić wykonane czynności.

Używanie protokołu zadania do sprawdzania: Po wprowadzeniu wielu zmian uprawnień, za pomocą komendy GRTOBJAUT, można przejrzeć protokół zadania, aby sprawdzić, czy zmiany zostały dokonane.

1. Wpisz DSPJOBLOG (Wyświetlenie protokołu zadania - Display Job Log).
2. Naciśnij klawisz **F10** (Wyświetlenie komunikatów szczegółowych).
3. Powinien pojawić się komunikat o zmianie uprawnień dla każdego obiektu w bibliotece. Podczas przeglądania komunikatów odznaczaj obiekty na swojej liście.

```
                Wyświetlenie wszystkich komunikatów
                     (Display All Messages)
                                                        System:   RCHASxxx
Zadanie. . :   QPADEV0010    Użytkownik. . :   JCHEIDEL     Numer . . . :   025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  Uprawnienie nadane użytkownikowi *PUBLIC dla obiektu CUSTMAS w typie obiektu CUSTLIB
    *FILE.
  Uprawnienie nadane użytkownikowi *PUBLIC dla obiektu CUSTMSGQ w typie obiektu CUSTLIB
    *MSGQ.
  Uprawnienie nadane do 2 obiektów. nie nadane do 0 obiektów. Częściowo nadane do 0
    obiektów.
  Uprawnienie do obiektu nadane.
7>> dspjoblog
```

Możliwy błąd	Rozwiązanie
Protokół zadania wskazuje, że dla niektórych obiektów biblioteki, uprawnienia nie zostały zmienione.	Aby uzyskać więcej informacji na temat komunikatu, skorzystaj z pomocy (**F1**). Aby osobno ustawić uprawnienia dla tych obiektów, użyj komendy EDTOBJAUT.

Teraz można ustawić uprawnienia publiczne dla nowych obiektów.

Ustawianie uprawnień publicznych dla nowych obiektów

W opisie biblioteki jest parametr o nazwie Tworzenie uprawnień (create authority - CRTAUT), który określa uprawnienia publiczne dla nowych obiektów tworzonych w bibliotece. Komendy tworzące obiekty domyślnie korzystają z uprawnień CRTAUT dla obiektów biblioteki. Parametr CRTAUT dla biblioteki powinien mieć taką samą wartość, jak uprawnienia publiczne dla większości obiektów istniejących w bibliotece.

1. Wpisz CHGLIB *nazwa_biblioteki* i naciśnij klawisz **F4** (Podpowiedź).
2. Naciśnij klawisz **F10** (Parametry dodatkowe).
3. W polu *Tworzenie uprawnień* wpisz nową wartość.

```
                      Zmiana biblioteki
                  (Change Library - CHGLIB)

Wypełnij pola i naciśnij Enter

Biblioteka . . . . . . . . . . . > CUSTLIB
Typ biblioteki . . . . . . . . .   *PROD
Tekst opisu. . . . . . . . . . .   'Rekordy klientów'


                           Parametry dodatkowe

Uprawnienie do tworzenia . . . .   *CHANGE
Kontrola tworzonego obiektu. . .   *SYSVAL
```

Jeśli parametr CRTAUT będzie miał wartość *SYSVAL, podczas tworzenia nowego obiektu w bibliotece, system skorzysta z aktualnych ustawień wartości systemowej QCRTAUT. Ustawienie dla każdej biblioteki określonych uprawnień CRTAUT, zabezpiecza przed przyszłymi zmianami w wartości systemowej QCRTAUT.

Teraz można pracować z bibliotekami dla grup i osobistymi.

Praca z bibliotekami dla grup i osobistymi

Profil użytkownika ma prawa do bibliotek dla grup i osobistych, które zostały utworzone podczas konfigurowania grup użytkowników i pojedynczych użytkowników.

Aby zmienić prawa własności do bibliotek dla grup na profile grupowe oraz prawa własności do bibliotek osobistych na pojedyncze profile użytkownika, należy skorzystać z poniższej procedury. W tym celu należy użyć komendy EDTOBJAUT.

Aby określić uprawnienia publiczne dla każdego nowo tworzonego obiektu, należy ustawić parametr Tworzenie uprawnień (Create Authority). W tym celu należy użyć komendy CHGLIB.

Przed rozpoczęciem tworzenia list autoryzacji, należy wykonać następujące czynności:

- Za pomocą Formularzy instalowania aplikacji i Formularzy opisywania biblioteki należy upewnić się, że dla wszystkich bibliotek aplikacji zostały ustanowione prawa własności oraz uprawnienia publiczne.
- Należy ustawić prawa własności i uprawnienia publiczne dla wszystkich tworzonych bibliotek grupy i osobistych.

Uwaga: Listę wszystkich bibliotek w systemie można uzyskać za pomocą komendy DSPOBJD *ALL *LIB *PRINT.

Tworzenie list autoryzacji

Po skonfigurowniu praw własności i uprawnień publicznych, można skonfigurować listy autoryzacji. Za pomocą informacji z Formularzy list autoryzacji należy utworzyć listy autoryzacji, które są potrzebne do zabezpieczania biblioteki. Korzystanie z komendy Tworzenie listy autoryzacji (Create Authorization List - CRTAUTL):

1. Wpisz CRTAUTL i naciśnij klawisz **F4** (Podpowiedź).
2. Podaj informacje z Formularza listy autoryzacji.
3. Naciśnij klawisz **F10** (Parametry dodatkowe).
4. Za pomocą parametru uprawnień określ uprawnienia publiczne dla obiektów, które są zabezpieczane przez listę.
5. Sprawdź komunikaty potwierdzenia.

```
                    Tworzenie listy autoryzacji
                (Create Authorization List - CRTAUTL)
Wypełnij pola i naciśnij Enter

Lista autoryzacji. . . . . .   custlst1
Tekst opisu. . . . . . . . . .   Czyszczone zbiory

                          Parametry dodatkowe

Uprawnienie  . . . . . . . . . . .   *ALL
```

Możliwy błąd	Rozwiązanie
Nazwa listy została niepoprawnie wpisana.	Po utworzeniu listy zmiana jej nazwy nie jest możliwa. Usuń listę (DLTAUTL) i spróbuj ponownie.
Zapomniano określić uprawnienia publiczne dla listy.	Użyj komendy Edycja listy autoryzacji (Edit Authorization List - EDTAUTL).

Teraz, za pomocą listy autoryzacji, można zabezpieczyć obiekty.

Zabezpieczanie obiektów za pomocą listy autoryzacji

Po utworzeniu listy autoryzacji, za pomocą komendy Edycja uprawnień dla obiektu (Edit Object Authority - EDTOBJAUT) można zabezpieczyć elementy wymienione w Formularzu listy autoryzacji:

1. Wpisz EDTOBJAUT i naciśnij klawisz **F4** (Podpowiedź).
2. Wypełnij ekran danymi i naciśnij klawisz **Enter**.
3. Na ekranie Edycja uprawnień dla obiektu (Edit Object Authority) podaj nazwę listy autoryzacji.
4. Jeśli uprawnienia publiczne dla obiektu pochodzą z listy autoryzacji, zmień je na wartość *AUTL.

5. Powtórz te czynności dla każdego obiektu z Formularza listy autoryzacji.

```
                          Edycja uprawnień dla obiektu
                            (Edit Object Authority)

Obiekt . . . . . :   ARFILE01        Właściciel . . . . . :   OWNAR
  Biblioteka . . . :     CUSTLIB     Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *FILE

Wprowadź zmiany w bieżących uprawnieniach i naciśnij Enter.

  Obiekt chroniony przez listę autoryzacji. . . . . .   CUSTLST1

                         Uprawnienie
Użytkownik  Grupa        do obiektu
OWNER                    *ALL
*PUBLIC                  *AUTL
```

Teraz mozna dodać użytkowników do listy autoryzacji .

Dodawanie użytkowników do listy autoryzacji.

Po zabezpieczeniu obiektów za pomocą listy autoryzacji, za pomocą komendy Edycja listy autoryzacji (Edit Authorization List - EDTAUTL) należy dodać użytkowników, wymienionych w Formularzu listy autoryzacji:

1. Wpisz EDTAUTL *nazwa_listy_autoryzacji*.
2. Na ekranie Edycja listy autoryzacji (Edit Authorization list) naciśnij klawisz **F6** (Dodawanie nowych użytkowników - Add new users).
3. Wpisz nazwy użytkowników lub grup oraz uprawnienia, które powinni mieć do elementów listy, a następnie naciśnij klawisz **Enter**.
4. Na liście powinni pojawić się nowi użytkownicy.

```
                    Dodawanie nowych użytkowników
                         (Add New Users)
Obiekt . . . . . :   WSLST1          Właściciel  . .
  Biblioteka . . . :     QSYS

Wpisz nowych użytkowników i naciśnij Enter.

             Uprawn.    Zarządz.
Użytkownik   do obiektu listą
QSECOFR     *CHANGE
```

Możliwy błąd	Rozwiązanie
Użytkownikom lub grupie nadano niewłaściwe uprawnienia do listy.	Uprawnienia można zmienić na ekranie Edycja listy autoryzacji (Edit Authorization List).
Do listy dodano niewłaściwego użytkownika lub grupę.	Użytkownika lub grupę można usunąć za pomocą komendy Usunięcie pozycji z listy autoryzacji (Remove Authorization List Entry - RMVAUTLE) lub obok uprawnień użytkownika na ekranie Edycja listy autoryzacji (Edit Authorization List) pozostawić puste miejsce.

Sprawdzanie

Za pomocą komendy Wyświetlenie listy autoryzacji (Display Authorization List - DSPAUTL) można wyświetlić listę uprawnień użytkownika do listy autoryzacji. Aby wyświetlić listę wszystkich obiektów chronionych przez listę autoryzacji, na ekranie należy nacisnąć klawisz **F15**.

Przed ustawieniem określonych uprawnień należy wykonać następujące czynności:

- za pomocą komendy CRTAUTL utworzyć listy autoryzacji wymagane przez aplikację,
- za pomocą komendy EDTOBJAUT zabezpieczyć obiekty za pomocą listy autoryzacji,
- za pomocą komendy EDTAUTL dodać użytkowników do list autoryzacji.

Ustawianie określonych uprawnień

W sekcji ″Ustawianie praw własności i uprawnień publicznych″ poznano sposób użycia komendy GRTOBJAUT do ustawiania uprawnień publicznych dla wszystkich obiektów w bibliotece, w oparciu o informacje z części 1 Formularza opisywania biblioteki. Teraz, za pomocą komendy Edycja uprawnień dla obiektu (Edit Object Authority - EDTOBJAUT), w oparciu o informacje z części 2 Formularza opisywania biblioteki należy ustawić uprawnienia szczegółowe do biblioteki lub obiektów w bibliotece.

W celu ustawienia uprawnień szczegółowych, należy zapoznać się z następującymi tematami:

- Ustawianie uprawnień szczegółowych do biblioteki.
- Ustawianie uprawnień szczegółowych dla obiektu.
- Ustawianie uprawnień dla więcej niż jednego obiektu.

Ustawianie uprawnień szczegółowych do biblioteki

Biblioteka to tak naprawdę specjalny rodzaj obiektu. Uprawnienia do biblioteki ustawia się za pomocą komendy EDTOBJAUT, tak samo jak uprawnienia do innych obiektów. Wszystkie biblioteki znajdują się w bibliotece QSYS dostarczanej przez firmę IBM. Ekrany w poniższych przykładach zawierają informacje z części 2 Formularza opisywania biblioteki dla biblioteki KONTRAKTY przedsiębiorstwa JKL Toy Company:

Lista uprawnień szczegółowych dla obiektów biblioteki				
Profil grupowy lub profil użytkownika	Nazwa obiektu	Rodzaj obiektu	Wymagane uprawnienia	Lista autoryzacji
DPTSM	KONTRAKTY	*LIB	*USE	
DPTMG	KONTRAKTY	*LIB	*USE	

1. Wpisz EDTOBJAUT i naciśnij klawisz **F4** (Podpowiedź).
2. Wypełnij ekran danymi i naciśnij klawisz **Enter**.

```
                        Edycja uprawnień dla obiektu
                    (Edit Object Authority - EDTOBJAUT)
Wypełnij pola i naciśnij Enter

Obiekt . . . . . . . . . . . . .   CONTRACTS
  Biblioteka . . . . . . . . . .     QSYS
Typ obiektu. . . . . . . . . . .   *LIB
```

3. Aby nadać uprawnienia użytkownikom, którzy nie znajdują się na liście, na ekranie Edycja uprawnień dla obiektu (Edit Object Authority), naciśnij klawisz **F6** (Dodawanie nowych użytkowników).
4. Naciśnij klawisz **Enter**.

```
                    Dodawanie nowych użytkowników
                          (Add New Users)
Obiekt . . . . . :   CONTRACTS       Właściciel . . . . . :   OWNCP
  Biblioteka . . . :     QSYS          Grupa podstawowa . . :   *NONE
Typ obiektu  . . . . :   *LIB


Wpisz nowych użytkowników i naciśnij Enter.

                   Uprawnienie
Użytkownik         do obiektu
DPTSM       *USE
DPTMG       *USE
```

5. Informacje na ekranie Edycja uprawnień dla obiektu (Edit Object Authority) powinny zgadzać się z informacjami z części 1 i 2 Formularza opisywania biblioteki.

```
                          Edycja uprawnień dla obiektu
                            (Edit Object Authority)

Obiekt . . . . . :   CONTRACTS       Właściciel . . . . . :   OWNCP
  Biblioteka . . . :     QSYS          Grupa podstawowa . . :   *NONE
Typ obiektu  . . . . :   *LIB

Wprowadź zmiany w bieżących uprawnieniach i naciśnij Enter.

  Obiekt chroniony przez listę autoryzacji  . . . . . .   *NONE

                         Uprawnienie
Użytkownik  Grupa        do obiektu
OWNCP                    *ALL
DPTSM                    *USE
DPTMG                    *USE
*PUBLIC     *EXCLUDE
```

Uprawnienia publiczne dla nowych użytkowników dla biblioteki (CRTAUT) nie pojawiają się na ekranie Edycja uprawnień dla obiektu (Edit Object Authority). Aby zobaczyć uprawnienia CRTAUT dla biblioteki, należy skorzystać z komendy Wyświetlenie biblioteki (Display Library - DSPLIB).

Powyższą procedurę można wykorzystać także do ustawienia uprawnień szczegółowych dla dowolnegoobiektu w systemie.

Teraz można ustawić uprawnienia szczegółowe dla obiektu.

Ustawianie uprawnień szczegółowych do obiektu

Procedura ustawiania uprawnień szczegółowych do obiektu w bibliotece aplikacji jest taka sama, jak procedura ustawiania uprawnień szczegółowych do biblioteki. W przykładzie wykorzystano informacje z części 2 Formularza opisywania biblioteki dla biblioteki COPGMLIB przedsiębiorstwa JKL Toy:

Tabela 62. Formularz opisywania biblioteki dla przedsiębiorstwa JKL Toy

Profil grupowy lub profil użytkownika	Nazwa obiektu	Rodzaj obiektu	Wymagane uprawnienia	Lista autoryzacji
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. Wpisz EDTOBJAUT i naciśnij klawisz **F4** (Podpowiedź).
2. Wypełnij ekran danymi i naciśnij klawisz **Enter**.
3. Na ekranie Edycja uprawnień dla obiektu (Edit Object Authority) podaj informacje o uprawnieniach i naciśnij klawisz **Enter**.

```
                          Edycja uprawnień dla obiektu
                            (Edit Object Authority)

Obiekt . . . . . :   COMSGQ01        Właściciel . . . . . :   OWNCO
  Biblioteka . . . :     COPGMLIB     Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *MSGQ

Wprowadź zmiany w bieżących uprawnieniach i naciśnij Enter.

  Obiekt chroniony przez listę autoryzacji  . . . . . .   *NONE

                         Uprawnienie
Użytkownik  Grupa        do obiektu
OWNCO                   *ALL
*PUBLIC                  *CHANGE
```

Teraz można ustawić uprawnienia dla więcej niż jednego obiektu.

Ustawianie uprawnień dla więcej niż jednego obiektu

W przykładach przedstawionych do tego momentu, do ustawiania uprawnień szczegółowych dla pojedynczego obiektu korzystano z komendy EDTOBJAUT. Do ustawienia ochrony dla wielu obiektów można użyć komendy Nadanie uprawnień dla obiektu (Grant Object Authority - GRTOBJAUT). W tym celu należy wpisać GRTOBJAUT i nacisnąć klawisz **F4** (Podpowiedź). Poniżej przedstawiono kilka przykładów dokonywania wielu zmian w uprawnieniach jednocześnie.

- Pola podane na poniższym ekranie, ustawiają uprawnienia publiczne dla wszystkich kolejek komunikatów w bibliotece CUSTLIB na *CHANGE.

```
                  Nadanie uprawnień dla obiektu
                (Grant Object Authority - GRTOBJAUT)
Wypełnij pola i naciśnij Enter

Obiekt . . . . . .   *all
  Biblioteka . . . . . .     custlib
Typ obiektu  . . . . . .   *msgq
Użytkownicy. . . . . .   *public
               + dla więcej
Uprawnienie. . . . . .   *change
```

- Pola podane na poniższym ekranie, nadają uprawnienia *ALL użytkownikowi AMES dla wszystkich plików, których nazwy rozpoczynają się od znaków WRK i znajdują się w bibliotece CUSTLIB.

```
                 Nadanie uprawnień dla obiektu
                   (Grant Object Authority)
Wypełnij pola i naciśnij Enter

Obiekt . . . . . .   WRK*
  Biblioteka . . . . . .     custlib
Typ obiektu  . . . . . .   *file
Użytkownicy. . . . . .   AMES
               + dla więcej
Uprawnienie. . . . . .   *all
```

W tym przykładzie użyto techniki określania parametrów, która nazywana jest nazewnictwem **ogólnym**. Wiele komend umożliwia podawanie pierwszych znaków parametru z następującym po nich znakiem gwiazdki (*). System wykonuje operację na każdym obiekcie, którego nazwa rozpoczyna się od tych znaków. Informacja elektroniczna dla komendy informuje, które parametry dopuszczają nazwy ogólne.

- Aby za pomocą listy autoryzacji ARLST1 zabezpieczyć wszystkie pliki, które rozpoczynają się od znaków AR oraz nadać im uprawnienia publiczne z listy, należy wykonać dwie czynności. Na poniższych ekranach pokazano wymagane czynności.

```
                Nadanie uprawnień dla obiektu
                  (Grant Object Authority)
Wypełnij pola i naciśnij Enter

Obiekt . . . . . . . . . . . . .   AR*
  Biblioteka . . . . . . . . . .     CUSTLIB
Typ obiektu  . . . . . . . . . .   *FILE

   :
Lista autoryzacjit . . . . . . .   ARLST1
```

```
                Nadanie uprawnień dla obiektu
                  (Grant Object Authority)
Wypełnij pola i naciśnij Enter

Obiekt . . . . . . . . . . . . .   AR*
  Biblioteka . . . . . . . . . .     CUSTLIB
Typ obiektu  . . . . . . . . . .   *FILE
Użytkownicy. . . . . . . . . . .   *PUBLIC
             + dla więcej
Uprawnienie. . . . . . . . . . .   *AUTL
             + dla więcej
```

Aby sprawdzić, czy system dokonał żądanych zmian uprawnień, należy skorzystać z komendy DSPJOBLOG, tak jak to opisano w sekcji ″Korzystanie z protokołu zadania do sprawdzania wykonanych czynności″.

Przed przejściem do sekcji ″Zabezpieczanie zbiorów wydruków″ należy skorzystać z komendy EDTOBJAUT lub GRTOBJAUT, aby ustawić uprawnienia szczegółowe z części 2 Formularza opisywania biblioteki.

Zabezpieczanie zbiorów wydruków

Po ustawieniu uprawnień szczegółowych można, korzystając z informacji w poniższych tematach, zabezpieczyć poufne zbiory wydruków:

- Tworzenie kolejki wyjściowej i kontrolowanie, kto może nią zarządzać.
- Przypisywanie do kolejki specjalnego zbioru wydruku.

Tworzenie kolejki wyjściowej

1. Wpisz CRTOUTQ (Tworzenie kolejki wyjściowej - Create Output Queue) i naciśnij klawisz **F4** (Podpowiedź).
2. Podaj nazwę kolejki wyjściowej i biblioteki.
3. Naciśnij klawisz **F10** (Parametry dodatkowe).
4. Przejdź do następnej strony i odszukaj informacje dotyczące ochrony kolejki wyjściowej.

```
                    Tworzenie kolejki wyjściowej
                   (Create Output Queue - CRTOUTQ)
Wypełnij pola i naciśnij Enter

Kolejka wyjściowa. . . . . . . . > NEWCP
  Biblioteka . . . . . . . . . .     CONTRACTS
Maks. wielkość zbioru buforow. :
  Liczba stron . . . . . . . . .   *NONE         Liczba, *NONE
  Czas rozpoczęcia . . . . . . .                Godzina
  Czas zakończenia . . . . . . .                Godzina
              + dla więcej
Porządek zbiorów w kolejce . . .   *FIFO
System zdalny  . . . . . . . . .   *NONE

   ⋮
Tekst opisu. . . . . . . . . . .   Kolejka nowych kontraktów
```

5. Na podstawie Formularza ochrony kolejki wyjściowej i stacji roboczej podaj informacje na temat tego, kto może korzystać i zarządzać kolejką wyjściową.
6. Naciśnij klawisz **Enter** i sprawdź komunikaty potwierdzające.

```
                    Tworzenie kolejki wyjściowej
                   (Create Output Queue - CRTOUTQ)
Wypełnij pola i naciśnij Enter


                           Parametry dodatkowe

Wyświetlenie dowolnego zbioru. .   *NO
Separatory zadań . . . . . . . .   0
Sterowane przez operatora. . . .   *NO
Kolejka danych . . . . . . . . .   *NONE
  Biblioteka . . . . . . . . . .
Uprawnienia do sprawdzania . . .   *OWNER
Uprawnienie. . . . . . . . . . .   *LIBCRTAUT
```

Możliwy błąd	Rozwiązanie
Zamiast klawisza **F10** naciśnięto klawisz **Enter**.	Aby wprowadzić dodatkowe informacje, skorzystaj z komendy Zmiana kolejki wyjściowej (Change Output Queue - CHGOUTQ).
Kolejkę wyjściową utworzono w niewłaściwej bibliotece.	Aby przenieść kolejkę do poprawnej biblioteki, użyj komendy Przeniesienie obiektu (Move Object - MOVOBJ).

Teraz do kolejki wyjściowej można przypisać zbiór wydruku.

Przypisywanie zbioru wydruku do kolejki wyjściowej

Po utworzeniu kolejki wyjściowej można do niej przypisać zbiór wydruku. Zbiór drukarkowy zazwyczaj steruje miejscem docelowym zbioru wydruku. Z pomocą dostawcy aplikacji należy sprawdzić nazwy i biblioteki zbiorów drukarkowych dla wydruków poufnych.

Jeśli nie ma dostępu do tych informacji, należy wykonać wydruk i wstrzymać go w kolejce wyjściowej. Aby odszukać nazwę zbioru drukarkowego, należy użyć opcji Atrybut na ekranie Praca ze zbiorami buforowymi (Work with Spooled Files). Zbiór drukarkowy pojawi się na ekranie w polu *Zbiór urządzenia*.

Aby zmienić miejsce docelowe (kolejkę wydruku) zbioru drukarkowego, należy skorzystać z komendy Zmiana zbioru drukarkowego (Change Printer File - CHGPRTF):

```
CHGPRTF FILE(nazwa_biblioteki/nazwa_zbioru_drukarkowego)
        OUTQ(nazwa_biblioteki/nazwa_kolejki_wyjściowej)
```

Wydruk zostanie skierowany do nowego miejsca przeznaczenia, gdy ktoś ponownie go zażąda. Aby zmienić miejsce docelowe dla zbioru buforowego, który jest już w kolejce wyjściowej, należy użyć opcji Zmiana na ekranie Praca ze zbiorami buforowymi (Work with Spooled Files).

Na przykład Sharon Jones w przedsiębiorstwie JKL Toy Company chce przypisać zbiór drukarkowy listy płac PRCLST1 do kolejki wyjściowej PRICEQ. Dlatego wpisuje:

```
CHGPRTF FILE(KONTRAKTY/PRCLST1) OUTQ(KONTRAKTY/PRICEQ)
```

Aby wszystkie wydruki listy płac przypisać do kolejki wyjściowej PRICEQ, Sharon powinna użyć ogólnej nazwy zbiorów drukarkowych:

```
CHGPRTF FILE(KONTRAKTY/PRCLST*) OUTQ(KONTRAKTY/PRICEQ)
```

Aby wszystkie nowe kontrakty skierować do kolejki wyjściowej NEWCP, Sharon powinna zmienić kolejkę wyjściową powiązaną z przykładowym dokumentem, który jest używany do tworzenia kontraktów.

Sprawdzanie

Najlepszym sposobem sprawdzenia strategii zabezpieczeń poufnych zbiorów wydruku, jest ich wydrukowanie. Należy sprawdzić, czy są kierowane do odpowiedniej kolejki wyjściowej. W tym celu należy wpisać się jako operator systemu i sprawdzić, czy można oglądać lub zmieniać zbiory w kolejce.

Przed zabezpieczeniem stacji roboczych, należy upewnić się, że:

- za pomocą komendy CRTOUTQ utworzono wszystkie kolejki wyjściowe wymienione w Formularzu ochrony kolejki wyjściowej i stacji roboczej,
- za pomocą komendy CHGPRTF zbiór wydruku przypisano do nowych kolejek wyjściowych.

Zabezpieczanie stacji roboczych

Po zabezpieczeniu zbioru wydruku należy zabezpieczyć stacje robocze. Stacje robocze można autoryzować tak samo, jak inne obiekty w systemie. Aby użytkownikom nadać uprawnienia do stacji roboczych, należy użyć komendy EDTOBJAUT.

Aby wpisać się do stacji roboczej, użytkownicy muszą mieć uprawnienia *CHANGE. Jeśli wartość systemowa QLMTSECOFR wynosi (0), szef ochrony oraz każda osoba z uprawnieniami *ALLOBJ może wpisać się do dowolnej stacji roboczej.

Jeśli wartość systemowa QLMTSECOFR wynosi (1), w celu ustawienia uprawnień do stacji roboczych, należy skorzystać z następujących wskazówek:

Użytkownicy, którzy mogą wpisywać się w stacji roboczej	Uprawnienia publiczne	Uprawnienia QSECOFR	Pojedyncze uprawnienia użytkownika
Wszyscy użytkownicy	*CHANGE	*CHANGE	Nie wymagane
Tylko wybrani użytkownicy	*EXCLUDE	Brak uprawnień	*CHANGE
Wybrani użytkownicy i użytkownicy z uprawnieniami do wszystkich obiektów	*EXCLUDE	*CHANGE	*CHANGE
Wszyscy użytkownicy z wyjątkiem użytkowników z uprawnieniami do wszystkich obiektów	*CHANGE	Brak uprawnień	Nie wymagane

Przed ograniczeniem dostępu do kolejki komunikatów operatora systemu, aby zabezpieczyć stacje robocze w oparciu o informacje z Formularza ochrony kolejki wyjściowej i stacji roboczej, należy użyć komendy EDTOBJAUT.

Ograniczanie dostępu do kolejki komunikatów operatora systemu

Ochronę można zwiększyć zabezpieczając zbiory wydruku, stacje robocze oraz ograniczając dostęp do kolejki komunikatów operatora systemu.

Opcje menu ASSIST dotyczące obsługi komunikatów umożliwiają użytkownikom korzystanie z klawisza funkcyjnego do wyświetlania kolejki komunikatów operatora systemu (QSYSOPR). Niepoprawne odpowiedzi na komunikaty operatora systemu mogą powodować problemy. Aby odpowiadać na komunikaty i usuwać je z kolejki komunikatów, użytkownicy muszą mieć uprawnienia *CHANGE. To uprawnienie powinni mieć tylko operatorzy systemu. Aby ustalić, kto powinien mieć uprawnienia *CHANGE do kolejki komunikatów operatora systemu, należy sprawdzić Formularz odpowiedzialności w systemie.

Aby to zrobić, należy użyć komendy EDTOBJAUT:

1. Wpisz EDTOBJAUT QSYSOPR *MSGQ i naciśnij klawisz **Enter**.
2. Aby wyświetlić szczegółowe informacje na temat uprawnień do obiektu, naciśnij klawisz **F11**.
3. Nadaj uprawnienia publiczne *OBJOPR, tak jak pokazano na przykładowym ekranie, i naciśnij klawisz **Enter**.

```
                  Edycja uprawnień dla obiektu
                    (Edit Object Authority)

Obiekt . . . . . :   QSYSOPR         Właściciel . . . . . :   QSYS
  Biblioteka . . . :     QSYS         Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :  *MSGQ

Wprowadź zmiany w bieżących uprawnieniach i naciśnij Enter.

  Obiekt chroniony przez listę autoryzacji  . . . . . .   *NONE

                       Uprawn.    ----------Obiekt-----------
Użytkownik   Grupa     do obiektu Oper Zarz. Istn. Zmia.  Odn.
*PUBLIC                USER DEF    X
```

4. System zmieni kolumnę *Uprawnienia do objektu* na wartość USER DEF (User defined - Definiowane przez użytkownika).
5. Aby wyświetlić szczegółowe informacje na temat uprawnień do obiektu, jeszcze raz naciśnij klawisz **F11**.
6. Nadaj uprawnienia publiczne *ADD, tak jak pokazano na przykładowym ekranie, i naciśnij klawisz **Enter**.

```
                  Edycja uprawnień dla obiektu
                    (Edit Object Authority)

Obiekt . . . . . :   QSYSOPR         Właściciel . . . . . :   QSYS
  Biblioteka . . . :     QSYS         Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :  *MSGQ

Wprowadź zmiany w bieżących uprawnieniach i naciśnij Enter.

  Obiekt chroniony przez listę autoryzacji  . . . . . .   *NONE

                       Uprawn.    ---------------Dane---------------
Użytkownik   Grupa     do obiektu Odcz. Dod. Zmiana  Usuw.   Urucham.
*PUBLIC                USER DEF          X
```

7. Za pomocą klawisza **F6** (Dodawanie użytkowników) dodaj użytkowników, którzy mają odpowiadać na komunikaty QSYSOPR. Nadaj im uprawnienia *CHANGE.

Uwaga: Nie należy nadawać uprawnień publicznych *EXCLUDE. Wszystkie zadania (i użytkownicy) muszą mieć możliwość dodawania komunikatów do kolejki QSYSOPR.

Aby upewnić się, że zakończono konfigurowanie ochrony zasobów, należy:

- za pomocą Formularzy listy autoryzacji i Formularzy opisywania biblioteki sprawdzić, czy ustanowiono ochronę dla wszystkich bibliotek aplikacji,
- sprawdzić Formularz ochrony kolejki wyjściowej i stacji roboczej, aby upewnić się, że zabezpieczono stacje robocze i utworzono specjalne kolejki wyjściowe,
- upewnić się, że ograniczono dostęp do kolejki komunikatów operatora systemu (QSYSOPR),
- zeskładować biblioteki aplikacji, według instrukcji dostarczonych z aplikacją; informacje o prawach własności i uprawnieniach publicznych składowane są razem z aplikacją,
- za pomocą komendy Składowanie danych ochrony (Save Security Data - SAVSECDTA) zeskładować utworzone informacje o ochronie; więcej informacji na temat składowania informacji o ochronie zawiera sekcja ″Składowanie informacji o ochronie″.

Teraz można rozpocząć testowanie konfiguracji ochrony.

Testowanie ochrony

W tym temacie opisano techniki testowania ochrony skonfigurowanej w systemie. W tym kontekście testowanie oznacza upewnienie się, że konfiguracja działa w zamierzony sposób. W temacie ″Monitorowanie ochrony″ omówiono w jaki sposób można szacować efektywność ochrony w swoim systemie.

Ochronę należy testować za każdym razem, gdy dokonywane są większe zmiany w systemie. Może to być dodawanie nowej aplikacji, ustawianie ochrony zasobów dla istniejącej aplikacji, dodawanie nowej grupy użytkowników lub zmienianie poziomu ochrony.

Przedstawione poniżej tematy zawierają informacje na temat metod testowania oraz diagnozowania problemów po wprowadzeniu zmian w ochronie:

- Testowanie profili użytkowników.
- Testowanie ochrony zasobów.

Testowanie profili użytkowników

Rozpoczynamy testowanie ochrony. Za każdym razem gdy w systemie tworzona jest nowa grupa, należy przetestować profil użytkownika. Należy przetestować jeden z pojedynczych profili, które zostały skopiowane z profilu grupowego.

- Czy można wpisać się za pomocą profilu użytkownika? Jeśli nie można się wpisać, należy sprawdzić protokół zadania, który został zapisany podczas nieudanej próby wpisywania się. Aby odszukać protokół zadania, należy skorzystać z opcji Praca z wydrukami (Work with Printer Output) z menu ASSIST.

  Poniżej przedstawiono najczęstsze problemy:

  – jeden z wymaganych obiektów, takich jak menu początkowe, biblioteka bieżąca lub program początkowy nie istnieje,
  – określona w opisie zadania lista bibliotek powoduje błędy; albo biblioteka nie istnieje albo do listy zapomniano dołączyć biblioteki QGPL i QTEMP,
  – użytkownik nie ma uprawnienia do tej stacji roboczej.
- Czy podczas wpisywania się na ekranie wyświetlane jest poprawne menu lub program początkowy?
- Co się dzieje podczas podawania na ekranie Wpisanie się (Sign On) menu początkowego lub biblioteki bieżącej? Jeśli użytkownik ma ustawione pole Ograniczone możliwości (Limited Capabilities) na Tak(YES), powinien pojawić się komunikat o błędzie.
- Czy po naciśnięciu klawisza ATTN pojawia się odpowiedni ekran?
- Czy wydruki przesyłane są do odpowiedniej drukarki? Jeśli nie, aby sprawdzić gdzie są przesyłane, należy użyć opcji Praca z wydrukami (Work with Printer Output) menu ASSIST. Aby określić, dlaczego wydruki kierowane są do innej drukarki, należy sprawdzić profil użytkownika i opis zadania.
- Czy użytkownik ma dostęp do wiersza komend?
- Czy użytkownik może wykonywać wymagane funkcje aplikacji bez pojawiania się błędów ochrony? Więcej szczegółów na ten temat zawiera sekcja ″Testowanie ochrony zasobów″.

- Czy użytkownik może wykonywać niezbędne zadania systemowe, takie jak zarządzanie drukarkami lub składowanie bibliotek?

Jeśli podczas wpisywania się za pomocą danego profilu system poprosił o zmianę hasła, po zakończeniu testowania hasło należy ponownie ustawić na nazwę profilu użytkownika:

1. Wpisz się za pomocą własnego profilu (z uprawnieniami szefa ochrony).
2. Wpisz CHGUSRPRF *nazwa_profilu* PASSWORD(*nazwa_profilu*) PWDEXP(*YES).

Po przetestowaniu profili użytkowników można przetestować ochronę zasobów.

Testowanie ochrony zasobów

Po przetestowaniu profili użytkowników, należy przetestować także ochronę zasobów. Podczas testowania ochrony zasobów, należy poszukać użytkowników:

- którzy nie mają odpowiednich uprawnień dla swoich zadań,
- którzy mają większe uprawnienia niż zamierzano im nadać.

Testowanie pod kątem niewystarczających uprawnień

Aby sprawdzić, czy profile użytkowników mają wystarczające uprawnienia, należy przetestować zarówno funkcje interaktywne jak i wsadowe.

Testowanie funkcji interaktywnych

Aby przetestować ochronę zasobów dla aplikacji, konieczne może być wpisywanie się za pomocą kilku różnych profili użytkowników. Zadaniem jest przetestowanie przykładowych użytkowników, aby upewnić się, że nadane uprawnienia są wystarczające.

- Przetestuj funkcje, które wymagają różnych poziomów uprawnień: przeglądanie, zmienianie i usuwanie.
- Przetestuj programy, a nie tylko menu. Wybranie opcji menu może nie być wystarczające do przetestowania uprawnień. Czasami system nie wykona operacji na pliku, dopóki użytkownik rzeczywiście nie będzie próbował wykonać operacji, takiej jak na przykład usuwanie rekordu. Sprawdzanie uprawnień następuje podczas otwierania pliku. To projekt aplikacji określa, kiedy system otwiera plik.
- Zachowaj zapis błędów ochrony i usuń je. Jeśli występuje błąd ochrony, należy sprawdzić komunikat pojawiający się na ekranie, który informuje, że użytkownik nie ma wystarczających uprawnień do wykonania operacji i który obiekt miał być użyty.

Testowanie funkcji wsadowych

- Za pomocą profili użytkowników, którzy będą wprowadzać zadania, uruchom przykładowe zadanie wsadowe aplikacji.
- Przetestuj zadania wsadowe, które wymagają różnych poziomów uprawnień: drukowanie informacji, zmienianie informacji lub czyszczenie plików na koniec miesiąca.
- W poszukiwaniu błędów ochrony sprawdź kolejkę komunikatów QSYSOPR i protokół QHST. Aby przejrzeć protokół QHST, należy użyć komendy DSPLOG. Komunikaty ochrony mają następujące numery: CPF2200, CPI2200, CPC2200, CPD2200, CPF4A00, CPI4A00, CPC4A00 i CPD4A00.

  Aby protokołować błędy uprawnień oraz inne zdarzenia związane z ochroną, można użyć także funkcji kontroli ochrony.

Testowanie pod kątem zbyt dużych uprawnień

Jeśli ochrona zasobów została skonfigurowana do zabezpieczania poufnych informacji, należy przetestować przykładowe profile użytkowników, aby upewnić się, że ochrona działa. W tym celu należy wpisać się za pomocą profilu użytkownika, który nie powinien mieć dostępu do poufnych plików.

- Czy jest dostęp do menu umożliwiającego dostęp do pliku?
- Co się dzieje po wybraniu opcji menu, która korzysta z pliku?

- Czy użytkownik ma dostęp do wiersza komend?
- Czy można uruchomić komendę powodującą wyświetlenie pliku, taką jak CPYF FROMFILE(*nazwa_pliku*) TOFILE(QSYSPRT)?
- Czy do obejrzenia pliku można użyć narzędzia do tworzenia zapytań?

Wyniki testu mogą wskazywać, że należy zmienić informacje o ochronie.

Zmienianie informacji o ochronie

Po zaplanowaniu ochrony systemu należy upewnić się, że plan będzie efektywny również po zmianach w przedsiębiorstwie.

Ten temat podkreśla prostotę jako główny cel przy projektowaniu ochrony. Jako wzorce dla pojedynczych użytkowników zaprojektowano grupy użytkowników. Próbowano korzystać z uprawnień publicznych, list autoryzacji oraz uprawnień do biblioteki a nie określonych pojedynczych uprawnień. Z takiego podejścia należy korzystać podczas zarządzania ochroną:

- przy dodawaniu nowej grupy użytkowników lub nowej aplikacji, należy korzystać z technik, których użyto do planowania ochrony,
- przy dokonywaniu zmian w ochronie, należy skorzystać z podejścia ogólnego, a nie tworzyć wyjątek rozwiązujący dany problem.

W temacie Komendy ochrony opisano, które komendy można wykorzystać do wyświetlania, zmieniania i usuwania informacji o ochronie.

Przedstawione poniżej tematy zawierają sugestie na temat obsługi różnych rodzajów zmian:

- Dodawanie nowego użytkownika do systemu.
- Tworzenie nowej grupy użytkowników.
- Zmienianie grupy użytkowników.
- Dodawanie nowej aplikacji.
- Dodawanie nowej stacji roboczej.
- Zmienianie zakresu odpowiedzialności użytkowników.
- Usuwanie użytkownika z systemu.

Komendy ochrony

Przedstawiona poniżej tabela pokazuje, które komendy można wykorzystać do pracy z obiektami ochrony. Komendy te można wykorzystać do wykonywania następujących zadań:

- Przeglądanie i pokazywanie informacji o ochronie.
- Zmienianie informacji o ochronie.
- Usuwanie informacji o ochronie.

Tabela 63. Komendy ochrony

Obiekt ochrony	Jak przeglądać	Jak zmieniać	Jak usuwać
Wartość systemowa	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	Nie może być usunięta
Opis zadania	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
Profil grupowy	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1],[2]

Tabela 63. Komendy ochrony (kontynuacja)

Obiekt ochrony	Jak przeglądać	Jak zmieniać	Jak usuwać
Profil użytkownika	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]
Uprawnienie do obiektu	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
Prawo własności do obiektu	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	Komenda CHGOBJOWN CHGOWN umożliwia odebranie praw poprzedniego właściciela.
Grupa podstawowa	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP grupa podstawowa ustawiona na *NONE
Kontrolowanie obiektu	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (ustawione na *NONE) CHGAUD
Lista autoryzacji	DSPAUTL DSPAUTLOBJ	EDTAUTL (uprawnienia użytkownika do listy) EDTOBJAUT (obiekt zabezpieczony przez listę) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (cała lista)[3] RMVAUTLE (usuwanie uprawnień użytkownika do listy) EDTOBJAUT (obiekt zabezpieczony przez listę) RVKOBJAUT

1. Do usuwania profilu firma IBM zaleca używanie opcji ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment). Za pomocą tej opcji można usunąć każdy obiekt, który należy do profilu, lub przypisać obiekt do nowego właściciela. Niektóre parametry komendy DLTUSRPRF umożliwiają usuwanie wszystkich obiektów, których właścicielem jest użytkownik, lub przypisanie ich do nowego właściciela. Nie można usunąć profilu, dopóki nie zostaną usunięte lub przepisane wszystkienależące do niego obiekty. Nie można także usunąć profilu, który jest grupą podstawową dla jakichkolwiek obiektów.
2. Nie można usunąć profilu grupowego, który ma jakichkolwiek członków. Aby wyświetlić listę członków grupy, należy użyć opcji *GRPMBR komendy DSPUSRPRF. Przed usunięciem profilu grupowego, w każdym pojedynczym profilu należy zmienić pole *Profil grupowy*.
3. Nie można usunąć listy autoryzacji, która jest używana do zabezpieczania obiektów. Aby wyświetlić obiekty, które są zabezpieczane przez listę, należy użyć komendy DSPAUTLOBJ. Za pomocą komendy EDTOBJAUT należy zmienić uprawnienia dla wszystkich obiektów, które są zabezpieczane przez listę.

Przeglądanie i pokazywanie informacji o ochronie

Za pomocą komendy wyświetlania (DSP) z opcją drukowania (*PRINT) można przeglądać informacje o ochronie. Na przykład, aby wyświetlić listę autoryzacji nazwaną MOJA_LISTA, należy wpisać DSPAUTL MOJA_LISTA *PRINT.

Niektóre komendy wyświetlania udostępniają opcje dla różnych rodzajów list. Na przykład podczas tworzenia pojedynczych profili użytkowników, do wyświetlenia wszystkich członków profilu grupowego, należy użyć opcji *GRPMBR komendy DSPUSRPRF. Aby sprawdzić, jakie listy dostępne są dla obiektów ochrony, należy skorzystać z podpowiedzi (**F4**) i informacji elektronicznych.

Komendy wyświetlania można używać do przeglądania informacji o ochronie na terminalu. Można także korzystać z komend Praca z ... (Work with... - WRK), które udostępniają więcej funkcji. Komendy Praca z ... (Work with...) udostępniają ekran listy. Można go używać do zmiany, usuwania i przeglądania informacji.

Do przeglądania lub pokazywania informacji można także używać komend ochrony wykorzystujących nazwy ogólne. Jeśli zostanie wpisane WRKUSRPRF WYD*,na ekranie Praca z rejestrowaniem użytkowników (Work with User

Enrollment) lub Praca z profilem użytkownika (Work with User Profile) pojawią się tylko profile rozpoczynające się od znaków *WYD*. Aby dowiedzieć się, które parametry dopuszczają nazwy ogólne, należy skorzystać z informacji elektronicznych.

Zmienianie informacji o ochronie

Za pomocą komendy Praca z ... (Work with... - WRK) lub Edytowanie ... (Edit... - EDT) interaktywnie można zmieniać informacje o ochronie. Można je przeglądać, zmieniać i ponownie przeglądać po zmianach.

Za pomocą komendy Zmiana ... (Change... - CHG) lub Nadanie ... (Grant... - GRT) można zmienić informacje o ochronie bez przeglądania ich przed i po dokonaniu zmiany. Ta metoda jest szczególnie przydatna do zmiany więcej niż jednego obiektu w tym samym czasie. NA przykład za pomocą komendy GRTOBJAUT można ustawić uprawnienia publiczne dla wszystkich obiektów w bibliotece (patrz sekcja “Ustawianie uprawnień publicznych do wszystkich obiektów w bibliotece.” na stronie 97).

Usuwanie informacji o ochronie

Niektóre rodzaje informacji o ochronie można usuwać za pomocą komend Praca z ... (Work with... - WRK) lub Edycja ... (Edit... - EDT). Do usuwania informacji o ochronie można także użyć komend Usunięcie ... (Delete... - DLT), Usuwanie ... (Remove... - RMV) i Odebranie ... (Revoke... - RVK). Często, zanim system pozwoli na usunięcie informacji o ochronie, trzeba spełnić pewne warunki. Uwagi z sekcji Komendy ochrony opisują niektóre z tych warunków.

Dodawanie nowego użytkownika do systemu

Jeśli do systemu trzeba dodać nowego użytkownika, należy skorzystać z następującej procedury:

1. Przypisz daną osobę do grupy użytkowników. W tym celu skorzystaj z Formularza opisywania grupy użytkowników.
2. Zadecyduj, czy nowy użytkownik musi wykonywać funkcje systemowe. Jeśli tak, to dodaj te informacje do Formularza odpowiedzialności w systemie.
3. Dodaj osobę do Formularza pojedynczego profilu użytkownika.
4. Przejrzyj Formularz odpowiedzialności w systemie oraz Formularz opisywania grupy użytkowników, aby określić, czy nowy użytkownik potrzebuje wartości innych niż te dla grupy.
5. Skopiuj profil grupowy lub profil członka grupy i utwórz profil użytkownika. Upewnij się, że ustawiono hasło jako wygasłe. (Więcej informacji zawiera sekcja ″Kopiowanie profilu grupowego.″)
6. Daj użytkownikowi kopię wytycznych ochrony.

Aby dowiedzieć się, jak utworzyć nową grupę, należy zapoznać się z sekcją ″Tworzenie nowej grupy użytkowników.″

Tworzenie nowej grupy użytkowników

Nowa grupa użytkowników może być potrzebna z kilku powodów:

- z systemu będą korzystać dodatkowe działy,
- okazało się, że grupy użytkowników powinny być bardziej specyficzne, tak aby spełniały wymagania ochrony zasobów,
- Przedsiębiorstwo zreorganizowało niektóre działy.

Aby utworzyć nową grupę użytkowników, należy:

1. Wypełnij Formularz opisywania grupy użytkowników korzystając z instrukcji z sekcji ″Planowanie grup użytkowników″.
2. Do diagramu aplikacji, bibliotek i grup użytkowników dodaj grupę użytkowników.
3. Ocenić, czy niektórzy członkowie grupy będą wykonywać funkcje systemowe. W tym celu zaktualizuj Formularz odpowiedzialności w systemie. (Więcej informacji na ten temat zawiera sekcja ″Określanie, kto powinien być odpowiedzialny za funkcje systemowe″).
4. Wypełnij Formularz pojedynczego profilu użytkownika, korzystając z informacji z Formularza opisywania grupy użytkowników oraz Formularza odpowiedzialności w systemie.

5. Utwórz bibliotekę grupy.
6. Utwórz opis zadania dla grupy.
7. Utwórz profil grupowy.

   Uwaga: Instrukcje na temat kroku piątego, szóstego i siódmego zawiera sekcja ″Konfigurowanie grup użytkowników″.
8. Utwórz pojedyncze profile użytkowników dla członków grupy. (Patrz sekcja ″Konfigurowanie pojedynczych użytkowników″).
9. Dla wszystkich aplikacji wymaganych przez grupę przygotuj Formularze opisywania biblioteki. Za pomocą technik opisanych w sekcji ″Konfigurowanie ochrony zasobów″ podejmij kroki niezbędne do nadania użytkownikom dostępu do obiektów aplikacji.
10. Daj wszystkim członkom grupy kopię wytycznych dotyczących ochrony.

Aby dowiedzieć się, jak zmienić grupę użytkowników, należy zapoznać się z sekcją ″Zmienianie grupy użytkowników″.

Zmienianie grupy użytkowników

Różne rodzaje zmian w charakterystykach grupy należy wykonywać na różne sposoby. Poniżej przedstawiono kilka przykładów zmian oraz sposób ich wprowadzania:

Zmienianie uprawnień grupowych

W pewnym momencie może okazać się, że wymagane przez grupę uprawnienia do obiektów nie są zgodne z początkowym planem. Wtedy należy wykonać następujące czynności:

1. Aby nadać użytkownikom odpowiedni dostęp do obiektów lub odpowiedniej listy autoryzacji, należy skorzystać z komendy Edycja uprawnień dla obiektu (Edit Object Authority - EDTOBJAUT). Sekcja “Ustawianie określonych uprawnień” na stronie 101 zawiera przykład wykonania tego zadania. Podczas nadawania uprawnień grupowych każdy członek grupy uzyskuje uprawienia do obiektu.
2. W przypadku nadania uprawnień grupowych do poufnych zasobów, można sprawdzić aktualnych członków grupy. Aby uzyskać listę członków grupy, należy skorzystać z komendy Wyświetlenie profilu użytkownika (Display User Profile) (DSPUSRPRF *nazwa_profilu_grupowego* *GRPMBR).

Zmienianie i dostosowywanie środowiska dla grupy

Czasem konieczna jest zmiana konfiguracji środowiska użytkownika dla członków grupy. Na przykład jeśli dział dostaje własną drukarkę, można ustawić ją jako drukarkę domyślną dla członków grupy użytkowników z danego wydziału. Inny przykład: jeśli w systemie instalowana jest nowa aplikacja, członkowie grupy mogą potrzebować innego menu początkowego.

Profil grupowy udostępnia wzorzec, który można skopiować w celu utworzenia pojedynczych profili dla członków grupy. Wartości konfiguracyjne profilu grupowego nie wpływają na pojedyncze profile użytkowników, po ich utworzeniu. Na przykład zmiana pola, takiego jak *Drukarka*, nie wpływa na członków grupy. Aby zmienić drukarkę, pole *Drukarka* należy zmienić w każdym pojedynczym profilu użytkownika.

Za pomocą ekranu Praca z profilami użytkowników (Work with User Profile)można zmienić parametr dla więcej niż jednego użytkownika jednocześnie. Przykład pokazuje zmianę kolejki wyjściowej dla wszystkich członków grupy:

1. Wpisz WRKUSRPRF *ALL i naciśnij klawisz **Enter**.
2. Jeśli pojawi się menu Praca z rejestrowaniem użytkowników (Work with User Enrollment), naciśnij klawisz **F21** (Wybór poziomu asysty), aby przejść do ekranu Praca z profilami użytkowników (Work with User Profile).

```
                     Praca z profilami użytkowników
                       (Work with User Profiles)

Wpisz opcje i naciśnij klawisz Enter.
  1=Utwórz  2=Zmień   3=Kopiuj   4=Usuń   5=Wyświetl
  12=Praca z obiekt. wg właścicieli

                Profil
  Opcja         użytkownika       Text
                HARRISOK         Harrison, Keith
2               HOGANR           Hogan, Richard
                JONESS           Jones, Sharon
2               WILLISR          Willis, Rose

   ⋮
                                                                Więcej...
Parametry dla opcji 1, 2, 3, 4 lub 5 albo komenda
===> PRTDEV(PRT02)
F3=Wyjście  F5=Odśwież   F12=Anuluj   F16=Powtórz ustaw na   F17=Ustaw na
F21=Wybór poziomu asysty   F24=Inne klawisze
```

3. Obok każdego profilu, który ma być zmieniony, wpisz **2** (Zmiana).
4. W wierszu parametrów, u dołu ekranu, wpisz nazwę parametru oraz jego nową wartość. Jeśli nie znasz nazwy parametru, naciśnij klawisz **F4** (Podpowiedź).
5. Naciśnij klawisz **Enter**. Pojawi się komunikat potwierdzający dla każdego zmienionego profilu.

   Chociaż zmiana pola konfiguracyjnego w profilu grupowym nie wpływa na członków grupy, to może być pomocna w przyszłości. Profil grupowy jest wzorcem podczas dodawania członków grupy. Jest także zapisem standardowych wartości pól dla grupy.

Nadawanie grupie dostępu do nowej aplikacji

Kiedy użytkownik grupy wymaga dostępu do nowej aplikacji, należy przeanalizować informacje o danej grupie oraz aplikacji. Poniżej przedstawiono zalecaną metodę:

1. Aby sprawdzić, które biblioteki wykorzystuje dana aplikacja, sprawdź Formularz opisywania aplikacji dla nowej aplikacji oraz diagram aplikacji, bibliotek i grup użytkowników. Dodaj te biblioteki do Formularza opisywania grupy.
2. Aktualizowanie diagramu aplikacji, bibliotek i grup użytkowników, w celu uwzględnienia nowych relacji między użytkownikiem grupy a aplikacją.
3. Jeśli początkowa lista bibliotek grupy powinna zawierać biblioteki, za pomocą komendy Zmiana opisu zadania (Change Job Description - CHGJOBD) zmień opis zadania grupy. W celu uzyskania pomocy podczas pracy z opisami zadań, zapoznaj się z sekcją “Tworzenie opisu zadania” na stronie 83.

   Uwaga: W przypadku dodawania bibliotek do początkowej listy bibliotek w opisie zadania, nie trzeba zmieniać profili użytkowników, które korzystają z tego opisu zadania. Podczas następnego wpisywania się użytkownika jego początkowa lista bibliotek automatycznie zostanie rozszerzona o te biblioteki.
4. Sprawdź, czy trzeba zmieniać program początkowy lub menu początkowe dla grupy, aby nadać dostęp do nowej aplikacji. Za pomocą komendy CHGUSRPRF zmień menu lub program początkowy dla każdego profilu użytkownika.
5. Przejrzyj Formularze opisywania biblioteki dla wszystkich bibliotek, które są używane przez aplikację. Określ, czy dostęp publiczny do tych bibliotek jest wystarczający dla potrzeb grupy. Jeśli nie, konieczne może być nadanie uprawnień grupowych do biblioteki, określonych obiektów lub list autoryzacji. Aby to zrobić, użyj komend Edycja uprawnień dla obiektu (Edit Object Authority - EDTOBJAUT) i Edycja listy autoryzacji (Edit Authorization List - EDTAUTL). (Więcej informacji na ten temat zawiera sekcja ″Konfigurowanie ochrony zasobów″).

Aby dodać aplikację do systemu, należy zapoznać się z sekcją ″Dodawanie nowej aplikacji.″

Dodawanie nowej aplikacji

Tak samo jak uważnie planowano ochronę aplikacji w systemie, tak samo należy zaplanować ochronę każdej nowej aplikacji. Należy wykonać następujące procedury:

1. Przygotuj dla aplikacji Formularz opisywania aplikacji i Formularz opisywania biblioteki.
2. Zaktualizuj diagram aplikacji, bibliotek i grup użytkowników.
3. Aby zadecydować, jak zabezpieczyć nową aplikację, wykonaj procedury opisane w sekcji ″Planowanie ochrony zasobów″.
4. Za pomocą metody opisanej w sekcji ″Planowanie instalowania aplikacji przygotuj Formularz instalowania aplikacji.
5. Oceń, czy zbiory wydruków z aplikacji są poufne i wymagają zabezpieczenia. Jeśli to konieczne, zaktualizuj Formularz ochrony kolejki wyjściowej i stacji roboczej.
6. Aby zainstalować i zabezpieczyć aplikację, wykonaj czynności opisane w sekcjach ″Ustawianie praw własności i uprawnień publicznych″ i ″Konfigurowanie ochrony zasobów″.

Przed dodaniem do systemu stacji roboczej należy zapoznać się z sekcją ″Dodawanie nowej stacji roboczej.″

Dodawanie nowej stacji roboczej

Podczas dodawania do systemu nowej stacji roboczej należy rozważyć wymagania ochrony:

1. Czy fizyczne położenie nowej stacji roboczej stwarza niebezpieczeństwo narażenia ochrony? (Więcej informacji na ten temat zawiera sekcja ″Planowanie ochrony fizycznej″).
2. Jeśli stacja robocza jest narażona na ryzyko, należy zaktualizować Formularz ochrony kolejki wyjściowej i stacji roboczej.
3. Nowe stacje robocze należy tworzyć normalnie, nadając im uprawnienia publiczne *CHANGE. Jeśli nie spełniają one wymagań dotyczących ochrony dla stacji roboczej, aby nadać im inne uprawnienia, należy skorzystać z komendy EDTOBJAUT.

Aby zmienić zakres odpowiedzialności użytkownika w systemie, należy zapoznać się z sekcją ″Zmienianie zakresu odpowiedzialności użytkownika″.

Zmienianie zakresu odpowiedzialności użytkownika.

Kiedy użytkownik otrzymuje w przedsiębiorstwie nowe zadanie lub zmienia zakres odpowiedzialności, należy ocenić, jak to wpłynie na jego profil użytkownika.

1. Czy użytkownik powinien należeć do innej grupy użytkowników? Aby zmienić grupę użytkowników, można użyć komendy CHGUSRPRF.
2. Czy trzeba zmienić jakieś wartości konfiguracyjne w profilu, takie jak drukarka lub menu początkowe? Do ich zmiany także można wykorzystać komendę CHGUSRPRF.
3. Czy uprawnienia do aplikacji nowego użytkownika grupy są wystarczające dla tej osoby?
   - Aby sprawdzić uprawnienia dla starych i nowych profili grupowych, należy skorzystać z komendy Wyświetlenie profilu użytkownika (Display User Profile - DSPUSRPRF).
   - Należy także sprawdzić uprawnienia pojedynczego profilu użytkownika.
   - Za pomocą komendy EDTOBJAUT należy wprowadzić wszystkie wymagane zmiany.
4. Czy użytkownik jest właścicielem jakichś obiektów? Czy należy zmienić prawa własności dla tych obiektów? W tym celu należy skorzystać z komendy Praca z obiektami wg właścicieli (Work with Objects by Owner - WRKOBJOWN).
5. Czy użytkownik wykonuje funkcje systemowe? Czy w związku z nowym zadaniem użytkownik musi wykonywać funkcje systemowe? Jeśli to konieczne, należy zaktualizować Formularz odpowiedzialności w systemie i zmienić profil użytkownika.

Aby dowiedzieć się, w jaki sposób usunąć użytkownika z systemu, należy zapoznać się z sekcją ″Usuwanie użytkownika z systemu.″

Usuwanie użytkownika z systemu

Jeśli ktoś odchodzi z przedsiębiorstwa, natychmiast należy usunąć z systemu jego profil użytkownika. Przed usunięciem profilu, należy usunąć lub przenieść prawa własności do każdego obiektu, którego właścicielem był dany profil. Aby to zrobić, można skorzystać z komendy WRKOBJOWN lub opcji **4** (Usunięcie) z ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment).

Po wybraniu dla profilu opcji **4** (Usunięcie) na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment), pojawią się dodatkowe ekrany, które umożliwiają obsługę wszystkich obiektów, których właścicielem jest użytkownik. Można wybrać opcję nadania wszystkich obiektów nowemu użytkownikowi lub obsługiwać je pojedynczo:

```
                Usuwanie użytkownika
                   (Remove User)

Użytkownik . . . . . :   HOGANR
Opis użytkownika . . . . . :   Dział sprzedaży i marketingu

Aby usunąć użytkownika, wpisz opcję i naciśnij Enter.

    1. Przypisz wszystkie obiekty tego użytkownika do nowego właściciela
    2. Usuń lub zmień właściciela wybranych obiektów należących do tego użytkownika
```

Jeśli wybrano opcję obsługi pojedynczych obiektów (opcja **2**), na ekranie zostanie wyświetlona lista wszystkich obiektów, których właścicielemjest użytkownik:

```
                Usuwanie użytkownika
                   (Remove User)

Użytkownik . . . . . :   HOGANR
Opis użytkownika . . . . . :   Dział sprzedaży i marketingu

Nowy właściciel. . . . . .                   Nazwa, F4 dla listy

Aby usunąć tego właściciela, usuń lub zmień właściciela wszystkich obiektów.
Wpisz opcje i naciśnij klawisz Enter.
  2=Zmień właściciela  4=Usuń   5=Wyświetl szczegóły

Opc  Obiekt        Biblioteka    Opis
 4   HOGANR        QUSRSYS       Hogan, Richard - kolejka komunikatów
 4   QUERY1        DPTWH         Kolejka magazynowa
```

Jeśli wybrano opcję usuwania obiektów, pojawi się ekran Potwierdzenie usunięcia (Confirm Delete). Po usunięciu obiektów można usunąć profil użytkownika. Ponownie zostanie wyświetlony ekran Praca z rejestrowaniem użytkowników (Work with User Enrollment), na którym będzie komunikat informujący, że system usunął użytkownika.

Składowanie informacji o ochronie

Ten temat zawiera przegląd sposobów składowania i odtwarzania informacji o ochronie. Jeśli planowane jest tworzenie i odtwarzanie kopii zapasowych systemu, należy rozważyć ochronę informacji, a także same informacje. Aby uzyskać pomoc przy projektowaniu pełnego planu tworzenia i odtwarzania kopii zapasowych, należy zapoznać się z tematem Centrum informacyjnego Składowanie, odtwarzanie i dostępność.

Przedstawione poniżej tematy opisują sposoby składowania i odtwarzania informacji o ochronie, które tworzone są podczas konfigurowania ochrony:

- Składowanie wartości systemowych.
- Składowanie profili grupowych i użytkowników.

- Składowanie opisów zadań.
- Składowanie informacji o ochronie zasobów.
- Korzystanie z profilu domyślnego właściciela (QDFTOWN).
- Odtwarzanie zniszczonej listy autoryzacji.

Składowanie wartości systemowych

Wartości systemowe przechowywane są są w bibliotece systemowej QSYS. Biblioteka QSYS składowana jest podczas:

- korzystania z komendy Składowanie systemu (Save System - SAVSYS),
- używania opcji składowania całego systemu z menu Składowanie (Save),
- używania opcji składowania informacji o systemie z menu Składowanie (Save),
- używania opcji składowania całego systemu z menu Uruchomienie składowania (Run Backup - RUNBCKUP).

Podczas odtwarzania całego systemu automatycznie odtwarzane są wartości systemowe.

Następnym krokiem jest ″Składowanie profili grupowych i użytkowników″.

Składowanie profili grupowych i użytkowników

Profile grupowe i użytkowników przechowywane są w bibliotece QSYS. Są składowane, kiedy używana jest komenda Składowanie systemu (Save System - SAVSYS) lub po wybraniu opcji menu do składowania całego systemu.

Profile grupowe i użytkowników można składować także za pomocą komendy Składowanie danych ochrony (Save Security Data - SAVSECDTA).

Profile użytkowników odtwarzane są za pomocą komendy Odtworzenie profili użytkowników (Restore User Profile - RSTUSRPRF). Zwykła sekwencja to:

1. odtworzenie systemu operacyjnego, co powoduje odtworzenie biblioteki QSYS,
2. odtworzenie profili użytkowników,
3. odtworzenie pozostałych bibliotek,
4. odtworzenie uprawnień do obiektów za pomocą komendy Odtwarzanie uprawnień (Restore Authority - RSTAUT).

Następnie należy zapoznać się z sekcją ″Składowanie opisów zadań″.

Składowanie opisów zadań

Podczas tworzenia opisu zadania podawana jest biblioteka, w której powinien być przechowywany. Firma IBM zaleca tworzenie opisów zadań w bibliotece QGPL.

Opisy zadań można składować, składując bibliotekę, w której się znajdują. Aby to zrobić, należy skorzystać z komendy Składowanie biblioteki (Save Library - SAVLIB). Opis zadania można składować także za pomocą komendy Składowanie obiektów (Save Object - SAVOBJ).

Zawartość biblioteki można odtworzyć za pomocą komendy Odtworzenie biblioteki (Restore Library - RSTLIB). Pojedynczy opis zadania można odtworzyć za pomocą komendy Odtworzenie obiektu (Restore Object - RSTOBJ).

Następnie należy zapoznać się z sekcją ″Składowanie informacji o ochronie zasobów″.

Składowanie informacji o ochronie zasobów

Ochrona zasobów, która definiuje, w jaki sposób użytkownicy mogą pracować z obiektami, składa się z różnych rodzajów informacji, które przechowywane są w różnych miejscach:

Tabela 64. Składowanie i odtwarzanie informacji o ochronie zasobów

Rodzaj informacji	Gdzie są przechowywane	Jak są składowane	Jak są odtwarzane
Uprawnienia publiczne	Z obiektem	Komenda SAVxxx [1]	Komenda RSTxxx [2]
Wartość kontroli obiektu	Z obiektem	Komenda SAVxxx [1]	Komenda RSTxxx [2]
Prawa własności dla obiektu	Z obiektem	Komenda SAVxxx [1]	Komenda RSTxxx [2]
Grupa podstawowa	Z obiektem	Komenda SAVxxx [1]	Komenda RSTxxx [2]
Lista autoryzacji	Biblioteka QSYS	Komenda SAVSYS lub SAVSECDTA	Komenda RSTUSRPRF USRPRF(*ALL)
Dowiązanie między obiektem a listą autoryzacji	Z obiektem	Komenda SAVxxx [1]	Komenda RSTxxx [2]
Uprawnienia prywatne	Z profilem użytkownika	Komenda SAVSYS lub SAVSECDTA	Komenda RSTAUT

1. Większość obiektów można składować za pomocą komendy SAVOBJ lub SAVLIB. Niektóre rodzaje obiektów, takie jak konfiguracyjne, mają specjalną komendę składowania.
2. Większość obiektów można odtwarzać za pomocą komendy RSTOBJ lub RSTLIB. Niektóre rodzaje obiektów, takie jak obiekty konfiguracyjne, mają specjalną komendę odtwarzania.

Jeśli potrzebne jest odzyskiwanie aplikacji lub całego systemu, wszystkie czynności należy ostrożnie zaplanować, łącznie z odtwarzaniem uprawnień do obiektów. Poniżej przedstawiono podstawowe kroki wymagane do odtworzenia informacji o ochronie zasobów dla aplikacji:

1. Jeśli to konieczne, odtwórz profile użytkowników, włącznie z profilami, które są właścicielami aplikacji. Za pomocą komendy RSTUSRPRF można odtworzyć wybrane lub wszystkie profile.
2. Odtwórz wszystkie listy autoryzacji, które są używane przez aplikację. Listy autoryzacji odtwarza się za pomocą komendy RSTUSRPRF USRPRF(*ALL).

   Uwaga: Spowoduje to odtworzenie z nośnika składowania wszystkich wartości profili użytkowników, łącznie z hasłami.
3. Za pomocą komendy RSTLIB lub RSTOBJ odtwórz biblioteki aplikacji. Powoduje to odtworzenie praw własności do obiektu, uprawnień publicznych oraz dowiązań między obiektami a listami autoryzacji.
4. Za pomocą komendy RSTAUT odtwórz uprawnienia prywatne do obiektów. Komenda RSTAUT odtwarza także uprawnienia użytkowników do list autoryzacji. Uprawnienia można odtworzyć dla określonego użytkownika lub dla wszystkich.

Informacje na temat odtwarzania obiektu oraz profilu właściciela, którego nie ma w systemie, zawiera sekcja ″Korzystanie z profilu właściciela domyślnego (QDFTOWN)″.

Korzystanie z profilu właściciela domyślnego (QDFTOWN)

W przypadku odtwarzania obiektu, którego profilu właściciela nie ma w systemie, system przenosi prawa własności do obiektu na profil domyślny, zwany QDFTOWN. Po odtworzeniu profilu właściciela lub po ponownym jego utworzeniu, za pomocą komendy Praca z obiektami wg właścicieli (Work with Object by Owner - WRKOBJOWN) można przenieść z powrotem prawa własności.

Informacje na temat odtwarzania listy autoryzacji zawiera sekcja ″Odtwarzanie zniszczonej listy autoryzacji″.

Odtwarzania zniszczonej listy autoryzacji

Jeśli lista autoryzacji, która chroni obiekt, zostanie zniszczona, dostęp do obiektu mają tylko ci użytkownicy, którzy mają uprawnienia specjalne dla wszystkich obiektów (*ALLOBJ).

Odtwarzanie zniszczonej listy autoryzacji obejmuje dwie czynności:

1. odtwarzanie użytkowników i ich uprawnień do listy autoryzacji,
2. odtwarzanie powiązań listy autoryzacji z obiektami.

Te czynności może wykonać użytkownik z uprawnieniami specjalnymi *ALLOBJ.

Krok 1: Odtwarzanie listy autoryzacji

Jeśli znane są uprawnienia użytkowników do listy autoryzacji, należy ją usunąć, utworzyć ponownie i dodać do niej użytkowników.

Jeśli nie są znane wszystkie uprawnienia do listy autoryzacji, za pomocą poniższych czynności należy ją odtworzyć z ostatnich taśm zeskładowanych za pomocą komendy SAVSYS lub SAVSECDTA:

1. Usuń zniszczoną listę autoryzacji:
   ```
   DLTAUTL AUTL(nazwa_listy_autoryzacji)
   ```
2. Odtwórz listę autoryzacji:
   ```
   Komenda RSTUSRPRF USRPRF(*ALL)
   ```
3. Za pomocą komendy Odtwarzanie uprawnień (Restore Authority - RSTAUT) dodaj do listy użytkowników.

Krok 2: Odtwarzanie powiązań obiektów z listą autoryzacji

Po odtworzeniu lub ponownym utworzeniu listy autoryzacji należy ustanowić dowiązania między listą a obiektami, które ma chronić:

1. Użyj komendy Odzyskiwanie pamięci (Reclaim Storage - RCLSTG). Komenda RCLSTG przypisuje obiekty, które były chronione przez zniszczoną listę autoryzacji, do domyślnej listy nazwanej QRCLAUTL.
2. Wyświetl obiekty, które są zabezpieczane przez listę autoryzacji QRCLAUTL:
   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```
3. Aby zabezpieczyć obiekty za pomocą odpowiedniej listy autoryzacji, użyj komendy GRTOBJAUT. Na przykład, aby zabezpieczyć plik ARWRK01 w bibliotece CUSTLIB za pomocą listy autoryzacji ARLST01, wpisz:
   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

Monitorowanie ochrony

Ten temat udostępnia podstawowe sugestie dotyczące monitorowania efektywności ochrony w systemie.

Monitorowanie ochrony zazwyczaj ma dwa podstawowe cele:

- zapewnienie, że zasoby przedsiębiorstwa są odpowiednio zabezpieczone,
- wykrywanie nieautoryzowanych prób dostępu do systemu oraz informacji przedsiębiorstwa.

Po zdecydowaniu, które zadania monitorowania należy wykonywać regularnie, należy przejrzeć instrukcję strategii ochrony oraz wytyczne ochrony.

Więcej informacji na temat monitorowania ochrony zawierają następujące tematy:

- Listy kontrolne dla monitorowania ochrony.
- Kontrolowanie ochrony.

Listy kontrolne dla monitorowania ochrony

Poniżej przedstawiono listy kontrolne, które dotyczą przeglądania różnych aspektów ochrony w systemie. Za ich pomocą można opracować plan.

Monitorowanie ochrony fizycznej

- Zabezpiecz nośniki składowania przed zniszczeniem lub kradzieżą.
- Ogranicz dostęp do stacji roboczych w miejscach publicznych. Za pomocą komendy DSPOBJAUT sprawdź, kto ma uprawnienia *CHANGE do stacji roboczych.

Monitorowanie wartości systemowych

- Sprawdź, czy ustawienia są zgodne z informacjami z Formularza wybierania wartości systemowych. Użyj komendy Wydruk atrybutów ochrony systemu (Print System Security Attributes - PRTSYSSECA).
- Przejrzyj decyzje dotyczące wartości systemowych, w szczególności podczas instalowania nowych aplikacji.

Monitorowanie profili grupowych

- Sprawdź, czy profile grupowe nie mają haseł. Aby sprawdzić, czy wszystkie profile grupowe mają hasła o wartości *NONE, użyj komendy DSPAUTUSR.
- Sprawdź, czy członkami grup są odpowiednie osoby. Aby wyświetlić listę członków grupy, użyj komendy DSPUSRPRF z opcją *GRPMBR.
- Sprawdź uprawnienia specjalne dla każdego profilu grupowego. Użyj komendy DSPUSRPRF. Jeśli ustawiony jest poziom ochrony 30, 40 lub 50, profile grupowe nie powinny mieć uprawnień *ALLOBJ.

Monitorowanie profili użytkowników

- Sprawdź, czy profile użytkowników należą do jednej z następujących kategorii:
  - profile użytkowników pracowników,
  - profile grupowe,
  - profile właścicieli aplikacji,
  - profile dostarczone przez firmę IBM (rozpoczynające się od litery Q).
- Jeśli przedsiębiorstwo przenosi pracownika lub pracownik odchodzi, usuń jego profil użytkownika. Aby automatycznie usunąć lub wyłączyć profil, użyj komendy Zmiana pozycji harmonogramu wygasania (Change Expiration Schedule Entry - CHGEXPSCDE).
- Poszukaj nieaktywnych profili i usuń je. Aby automatycznie wyłączać profile po pewnym czasie bezczynności, użyj komendy Analiza aktywności profilu (Analyze Profile Activity - ANZPRFACT).
- Określ, którzy użytkownicy mają hasła takie same, jak ich nazwa profilu użytkownika. W tym celu użyj komendy Analiza domyślnych haseł (Analyze Default Passwords - ANZDFTPWD). Skorzystaj z opcji tej komendy, która wymusza na użytkownikach zmianę hasła podczas następnego wpisywania się do systemu.

  Uwaga: Nie należy usuwać z systemu żadnych profili dostarczonych przez firmę IBM. Takie profile rozpoczynają się od litery Q.
- Sprawdź, kto ma klasę użytkownika inną niż *USER i dlaczego. Aby uzyskać listę wszystkich użytkowników, ich klas oraz uprawnień specjalnych, skorzystaj z komendy Drukowanie profilu użytkownika (Print User Profile - PRTUSRPRF). Porównaj te informacje z Formularzem odpowiedzialności w systemie.
- Kontroluj, które profile użytkowników mają wartość *NO w polu *Ograniczenie możliwości*.

Monitorowanie obiektów krytycznych

- Sprawdź, kto ma dostęp do obiektów krytycznych. Aby monitorować obiekty, użyj komendy Drukowanie uprawnień prywatnych (Print Private Authorities - PRTPVTAUT) oraz Drukowanie obiektów z uprawnieniami publicznymi (Print Publicly Authorized Objects - PRTPUBAUT). Jeśli dostęp ma grupa, za pomocą opcji *GRPMBR komendy DSPUSRPRF sprawdź członków tej grupy.
- Sprawdź, kto może korzystać z aplikacji, które umożliwiają dostęp do obiektów przez inne metody ochrony, takie jak adoptowanie ochrony. W tym celu użyj komendy Drukowanie obiektów adoptujących (Print Adopting Objects - PRTADPOBJ).

Monitorowanie nieautoryzowanego dostępu

- Poinstruuj operatorów systemu, aby zwracali uwagę na komunikaty ochrony w kolejce komunikatów QSYSOPR. W szczególności niech powiadamiają szefa ochrony o wielokrotnych próbach nieudanego wpisywania się. Komunikaty ochrony są z zakresu od 2200 do 22FF i od 4A00 do 4AFF. Mają one przedrostki CPF, CPI, CPC i CPD.
- Skonfiguruj kontrolę ochrony tak, aby nieautoryzowane próby dostępu do obiektów były protokołowane.

Następnie należy zapoznać sie z sekcją Kontrolowanie ochrony.

Kontrolowanie ochrony

Podczas monitorowania ochrony system operacyjny może protokołować zdarzenia ochrony, które miały miejsce. Takie zdarzenia są zapisywane w specjalnych obiektach systemowych, zwanych **dziennikami**. Dzienniki można skonfigurować do zapisywania różnych rodzajów zdarzeń systemowych, takich jak zmiana wartości systemowej lub profilu użytkownika lub niepomyślne próby dostępu do obiektu. Przedstawione poniżej wartości sterują tym, które zdarzenia mają być protokołowane:

- wartość systemowa Sterowanie kontrolą (QAUDCTL),
- wartość systemowa Poziom kontroli (QAUDLVL),
- wartość Poziom kontroli (AUDLVL) w profilach użytkowników,
- wartość Kontrola obiektu (OBJAUD) w profilach użytkowników,
- wartość Kontrola obiektu (OBJAUD) w obiektach.

Informacje z kronik kontroli używane są do:

- wykrywania prób naruszeń ochrony,
- planowania migrowania do wyższych poziomów ochrony,
- monitorowania użycia wrażliwych obiektów, takich jak poufne pliki i zbiory.

Do przeglądania informacji kronik kontroli dostępne są specjalne komendy.

Formularze planowania podstawowej ochrony systemu

Formularze można kopiować lub drukować z przeglądarki.

Aby wydrukować wszystkie informacje na temat ochrony, należy wybrać prawy panel i kliknąć ikonę PDF na banerze Centrum informacyjnego.

Aby wydrukować pojedynczy formularz planowania, należy kliknąć odsyłacz odpowiadający formularzowi, który ma być wydrukowany. Należy kliknąć prawy panel, a następnie w przeglądarce ikonę Drukuj. Spowoduje to wydrukowanie wybranego formularza.

Poniżej przedstawiono pełną listę wszystkich formularzy planowania, które są wymagane do pomyślnego zaplanowania, a następnie korzystania z podstawowej ochrony systemu:

- Formularz planowania ochrony fizycznej
- Formularz opisywania aplikacji
- Formularz konwencji nazewnictwa
- Formularz opisywania biblioteki
- Formularz wybierania wartości systemowych
- Formularz odpowiedzialności w systemie
- Formularz identyfikowania grupy użytkowników
- Formularz opisywania grupy użytkowników
- Formularz pojedynczego profilu użytkownika
- Formularz list autoryzacji
- Formularz ochrony kolejki wyjściowej i stacji roboczej
- Formularz instalowania aplikacji

Formularz planowania ochrony fizycznej

Tabela 65. Formularz planowania ochrony fizycznej

Formularz planowania ochrony fizycznej	
Przygotowany przez:	Data:

Tabela 65. Formularz planowania ochrony fizycznej (kontynuacja)

Instrukcje • Instrukcje dotyczące tego formularza zawiera sekcja ″Planowanie ochrony zasobów.″ • Tego formularza należy użyć do opisania wytycznych ochrony, które są związane z fizycznym położeniem jednostki systemowej oraz podłączonych urządzeń. • Informacji podanych w tym formularzu nie trzeba wpisywać w systemie.	
Jednostka systemowa:	
Opis wytycznych ochrony, w celu zabezpieczenia jednostki systemowej (takich jak pokój zamknięty):	
Jaka pozycja kluczyka jest zazwyczaj wykorzystywana?	
Gdzie jest przechowywany klucz?	
Pozostałe komentarze dotyczące jednostki systemowej:	
Nośniki składowania i dokumentacja:	
Gdzie w siedzibie firmy przechowywane są taśmy kopii zapasowej?	
Gdzie poza siedzibą firmy przechowywane są taśmy kopii zapasowej?	
Gdzie przechowywane są hasła szefa ochrony, serwisu i narzędzi DST?	
Gdzie jest przechowywana ważna dokumentacja systemowa, taka jak numer seryjny i konfiguracja?	

Formularz planowania ochrony fizycznej			Część 2 z 2
Dodatkowe instrukcje dla części 2 • Poniżej należy wymienić stacje robocze lub drukarki, których położenie może powodować ryzyko naruszenia ochrony. Należy wskazać, jakie środki zaradcze zostaną podjęte. Dla drukarek, w kolumnie *Ryzyko naruszenia ochrony* należy podać przykłady poufnych wydruków. • Jeśli urządzenia lokalne mają być konfigurowane automatycznie, do czasu zainstalowania systemu mogą nie być znane nazwy stacji roboczych i drukarek. Jeśli podczas przygotowywania tego formularza nazwy nie są znane, należy podać opis (taki jak położenie), a nazwy dodać później.			
Ochrona fizyczna stacji roboczych i drukarek			
Nazwa stacji roboczej lub drukarki	Jej położenie lub opis	Ryzyko naruszenia ochrony	Podejmowane środki zabezpieczające

Formularz opisywania aplikacji

Tabela 66. Formularz opisywania aplikacji

Formularz opisywania aplikacji	
Przygotowany przez:	Data:

Tabela 66. Formularz opisywania aplikacji (kontynuacja)

Instrukcje • Instrukcje dotyczące tego formularza zawierają sekcje ″Opisywanie aplikacji″ i ″Planowanie ochrony zasobów.″ • Dla każdej aplikacji należy przygotować oddzielny formularz. • Informacji podanych w tym formularzu nie trzeba wpisywać w systemie.	
Nazwa aplikacji:	Nazwa skrócona:
Krótki opis aplikacji:	
Nazwa menu podstawowego:	Biblioteka:
Nazwa programu początkowego:	Biblioteka:
Lista bibliotek używana przez aplikację, zarówno dla plików, jak i programów:	
Zdefiniuj cele ochrony aplikacji, np. czy zawiera poufne informacje:	

Formularz konwencji nazewnictwa

Tabela 67. Formularz konwencji nazewnictwa

Formularz konwencji nazewnictwa	
Przygotowany przez:	Data:
Instrukcje • Instrukcje dotyczące tego formularza zawiera sekcja ″Opisywanie aplikacji.″ • Informacji podanych w tym formularzu nie trzeba wpisywać bezpośrednio w systemie. • Za pomocą tego formularza należy opisać sposób nadawania nazw obiektom w systemie. Należy podać przykład dla każdego sposobu.	
Rodzaj obiektu	**Konwencja nazewnictwa**
Profile grupowe	
Profile użytkowników	
Listy autoryzacji	
Biblioteki	
Pliki	
Kalendarze	
Urządzenia	
Taśmy	

Formularz opisywania biblioteki

Tabela 68. Formularz opisywania biblioteki

Formularz opisywania biblioteki	Część 1 z 2
Przygotowany przez:	Data:
Instrukcje: • Instrukcje dotyczące tego formularza zawiera sekcja ″Planowanie ochrony użytkowników″ i ″Planowanie ochrony zasobów.″ • Za pomocą tego formularza należy opisać główne biblioteki oraz zdefiniować wymaganą przez nie ochronę zasobów. • Dla każdej głównej biblioteki w systemie należy wypełnić jeden formularz. • Informacje dotyczące wprowadzania danych z tego formularza zawiera sekcja ″Konfigurowanie ochrony zasobów.″	
Nazwa biblioteki:	Nazwa opisowa (tekst):

Tabela 68. Formularz opisywania biblioteki (kontynuacja)

Krótki opis funkcji tej biblioteki:	
Zdefiniuj cele ochrony biblioteki, np.czy zawiera poufne informacje:	
Uprawnienia publiczne do biblioteki:	
Uprawnienia publiczne dla obiektów w bibliotece:	
Uprawnienia publiczne dla nowych obiektów (CRTAUT):	
Właściciel biblioteki:	

Formularz opisywania biblioteki				Część 2 z 2
Przygotowany przez:			Data:	
Nazwa biblioteki:				
Dodatkowe instrukcje dla części 2: • W poniższej tabeli należy wypisać wszystkich użytkowników lub obiekty wymagające uprawnień specjalnych. • Należy określić rodzaj wymaganych uprawnień: *ALL, *CHANGE, *USE lub *EXCLUDE.				
Lista uprawnień specjalnych do obiektów biblioteki				
Profil grupowy lub użytkownika	Nazwa obiektu	Rodzaj obiektu	Wymagane uprawnienia	Lista autoryzacji

Formularz wybierania wartości systemowych

Tabela 69. Formularz wybierania wartości systemowych

Formularz wybierania wartości systemowych		Część 1 z 2
Przygotowany przez:		Data:
Instrukcje • Instrukcje dotyczące tego formularza zawiera sekcja ″Planowanie ogólnej strategii ochrony.″ • Za pomocą tego formularza należy zapisać ustawienia wartości systemowych wpływających na ochronę i konfigurację. • Aby wprowadzić część 1 tego formularza, należy skorzystać z opcji **1** z menu menu SETUP.		
Wartości ekranu Zmiana opcji systemu (Change System Options)		
Wartość systemowa/atrybut sieciowy	**Zalecany wybór**	**Wybór użytkownika**
Nazwa systemu		
Separator daty (QDATSEP)		
Format daty (QDATFMT)		
Separator godziny (QTIMSEP)		
Format nazewnictwa dla nowych urządzeń (QDEVNAMING)	1 (system iSeries)	
Drukarka systemowa (QPRTDEV)		
Poziom ochrony (QSECURITY)	40	

Tabela 69. Formularz wybierania wartości systemowych (kontynuacja)

Umożliwienie szefom ochrony wpisywania się z każdej stacji roboczej (QLMTSECOFR)	N	
Składowanie informacji rozliczeniowych zadania dotyczących zakończonych wydruków (QACGLVL)	N (*NONE)	

Formularz wybierania wartości systemowych		Część 2 z 2
Dodatkowe instrukcje dla części 2 • Więcej informacji na temat części 2 tego formularza, zawiera sekcja ″Ustawianie wartości systemowych.″ • Aby wprowadzić informacje z części 2, należy skorzystać z komendy Praca z wartościami systemowymi (Work With System Value - WRKSYSVAL).		
Wartości systemowe dotyczące ochrony		
Wartość systemowa	**Zalecany wybór**	**Wybór użytkownika**
Interwał czasu nieaktywności zadania (QINACTITV)	Od 30 do 60	
Kolejka komunikatów nieaktywnego zadania (QINACTMSGQ)	*DSCJOB	
Ograniczanie sesji urządzeń (QLMTDEVSSN)	1 (YES)	
Działanie podejmowane po nieudanych próbach wpisywania się (QMAXSGNACN)	3 (wyłączenie obydwu)	
Maksymalna, dozwolona liczba prób wpisania się (QMAXSIGN)	Od 3 do 5	
Okres ważności hasła (QPWDEXPITV)	Od 30 do 60	
Maksymalna długość hasła (QPWDMAXLEN)	8	
Minimalna długość hasła (QPWDMINLEN)	6	
Wymaganie różnych haseł (QPWDRQDDIF)	7 (6 unikalnych haseł)	
Pozostałe wartości systemowe		
Wartość systemowa	**Zalecany wybór**	**Wybór użytkownika**
Interwał czasu przed przerwaniem odłączonych zadań (QDSCJOBITV)	300	
Uwaga: Istnieje możliwość ustawienia innych wartości systemowych związanych z ochroną. Rozdział trzeci podręcznika *Ochrona* (SC85-0124-04) zawiera pełną listę wartości systemowych związanych z ochroną oraz zalecenia z nimi związane.		

Formularz odpowiedzialności w systemie

Tabela 70. Formularz odpowiedzialności w systemie

Formularz odpowiedzialności w systemie	
Przygotowany przez:	Data:

Tabela 70. Formularz odpowiedzialności w systemie (kontynuacja)

Instrukcje: • Instrukcje dotyczące tego formularza zawiera sekcja ″Planowanie pojedynczych profili użytkowników.″ • Tego formularza należy użyć dla użytkowników, którzy mają klasę użytkownika inną niż *USER. • Informacje z tego formularza należy przenieść do kolumny *Klasa użytkownika* w Formularzu pojedynczego profilu użytkownika.
Kto jest głównym szefem ochrony? Kto jest szefem ochrony zajmującym się składowaniem?

Nazwa profilu	Nazwa użytkownika	Klasa	Uwagi

Formularz identyfikowania grupy użytkowników

Tabela 71. Formularz identyfikowania grupy użytkowników

Formularz identyfikowania grupy użytkowników	
Przygotowany przez:	Data:

Instrukcje:
- Instrukcje dotyczące tego formularza zawiera sekcja ″Planowanie grup użytkowników.″
- Ten formularz pomaga identyfikować grupy użytkowników, którzy mają podobne wymagania odnośnie aplikacji.
  1. U góry formularza należy wymienić główne aplikacje.
  2. W kolumnie po lewej stronie należy wymienić użytkowników.
  3. Dla każdego użytkownika należy zaznaczyć wymaganą aplikację.
- Informacji podanych w tym formularzu nie trzeba wpisywać w systemie.

		Wymagany dostęp do aplikacji						
Nazwa użytkownika	Dział	Aplik:	Aplik:	Aplik:	Aplik:	Aplik:	Aplik:	Aplik:

Uwaga:
- W przypadku *łagodnego* środowiska ochrony, aby zaznaczyć wymagane przez użytkownika aplikacje, należy użyć znaku **X**.
- W przypadku *ścisłego* środowiska ochrony, należy użyć liter **Z** (zmiana) i **P** (przeglądanie), aby określić, *w jaki sposób* aplikacje mają być używane.

Formularz opisywania grupy użytkowników

Tabela 72. Formularz opisywania grupy użytkowników

Formularz opisywania grupy użytkowników	Część 1 z 2
Przygotowany przez:	Data:
Instrukcje dla części 1 • Instrukcje dotyczące przygotowywania tego formularza zawiera sekcja ″Planowanie grup użytkowników.″ • Informacje dotyczące wprowadzania danych z tego formularza zawiera sekcja ″Konfigurowanie ochrony użytkowników.″ • Dla każdej grupy, która będzie w systemie, należy przygotować oddzielny formularz. • Aby utworzyć opis zadania dla grupy, należy użyć komendy Tworzenie opisu zadania (Create Job Description - CRTJOBD). Opis zadania zawiera początkową listę bibliotek dla grupy.	
Nazwa profilu grupowego: Opis grupy:	
Podstawowa aplikacja dla grupy: Pozostałe aplikacje wymagane przez grupę:	
Biblioteki wymagane przez grupę. Zaznacz (✓) każdą bibliotekę, która powinna znaleźć się na początkowej liście bibliotek dla tej grupy:	
Uwaga: Aby sprawdzić, które biblioteki wykorzystuje dana aplikacja, przejrzyj Formularz opisywania aplikacji dla każdej aplikacji, która została wymieniona w poprzedniej sekcji.	

Formularz opisywania grupy użytkowników		Część 2 z 2
Dodatkowe instrukcje dla części 2 • Przedstawiona poniżej tabela zawiera listę wszystkich pól, które zostaną wyświetlone na ekranie Tworzenie profilu użytkownika (Create User Profile). Pola są podzielone na dwie grupy: te, dla których trzeba wybrać wartość oraz te, dla których firma IBM zaleca wartości domyślne. • Aby wprowadzić do systemu informacje z tej części formularza, należy skorzystać z ekranu Praca z profilami użytkowników (Work with User Profiles) lub z komendy Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF).		
Dla poniższych pól profilu grupowego, należy wybrać wartości:		
Nazwa pola	**Zalecany wybór**	**Wybór użytkownika**
Nazwa profilu grupowego (użytkownik)		
Hasło	*NONE	
Klasa użytkownika (Rodzaj użytkownika)	*USER	
Biblioteka bieżąca (Biblioteka domyślna)	*taki sam jak nazwa profilu grupowego*	
Wywoływany program początkowy (program wpisywania się)		
Biblioteka programu początkowego		
Menu początkowe (pierwsze menu)		
Biblioteka menu początkowego		
Ograniczenie możliwości (ograniczenie użycia wiersza komend)	*YES	
Tekst (opis użytkownika)		
Opis zadania	*taki sam jak nazwa profilu grupowego*	
Biblioteka opisu zadania		
Nazwa profilu grupowego (grupa użytkowników)	*NONE	

Drukarka (drukarka domyślna)		
Kolejka wyjściowa	*DEV	
Uwaga: Te pola ułożone są w takiej kolejności, w jakiej pojawiają się na ekranie Tworzenie profilu użytkownika (Create User Profile) (po użyciu klawisza F4).		
Dla pól przedstawionych poniżej należy użyć wartości domyślnych:		
Kod rozliczeniowy	Buforowanie klawiatury	Uprawnienia publiczne
Poziom asysty	ID języka	Ustawienie hasła jako wygasłe
Program klawisza ATTN	Ograniczenie sesji urządzeń	Kolejność sortowania
Identyfikator CCSID	Pamięć maksymalna	Uprawnienia specjalne
ID kraju lub regionu	Kolejka komunikatów	Środowisko specjalne
Wyświetlenie informacji wpisania	Okres ważności hasła	Status
Hasło do dokumentu	Ograniczenie priorytetu	Opcje użytkownika
Uwaga: Pola na liście ułożone są w porządku alfabetycznym.		

Formularz pojedynczego profilu użytkownika

Tabela 73. Formularz pojedynczego profilu użytkownika

Formularz pojedynczego profilu użytkownika						
Przygotowany przez:			Data:			
Instrukcje: • Instrukcje dotyczące przygotowywania tego formularza zawiera sekcja ″Planowanie pojedynczych profili użytkowników.″ • Za pomocą tego formularza należy zapisać informacje na temat pojedynczych użytkowników systemu. Dla każdej grupy użytkowników (profilu grupowego), która jest w systemie, należy wypełnić jeden formularz. • Dla dodatkowych pól, które mają być określone dla pojedynczego użytkownika, należy wykorzystać puste kolumny po prawej stronie. • Informacje dotyczące wprowadzania danych z tego formularza zawiera sekcja ″Konfigurowanie pojedynczych użytkowników.″						
Nazwy profili grupowych:						
Właściciel tworzonych obiektów:			Uprawnienia grupy do tworzonych obiektów:			
Rodzaj uprawnień grupy:						
Utwórz jedną pozycję dla każdego członka grupy:						
Profil użytkownika	Tekst (opis)	klasa użytkownika	Ograniczenie możliwości			

Formularz list autoryzacji

Tabela 74. Formularz list autoryzacji

Formularz list autoryzacji					
Przygotowany przez:			Data:		
Instrukcje • Instrukcje dotyczące tego formularza zawiera sekcja ″Planowanie ochrony zasobów.″ • Dla każdej listy autoryzacji należy przygotować jeden formularz. • Na formularzu należy wypisać obiekty, które chroni lista, a do których mają dostęp grupy i pojedynczy użytkownicy. • Informacje dotyczące wprowadzania danych z tego formularza zawiera sekcja ″Konfigurowanie ochrony zasobów.″					
Nazwa listy autoryzacji:					
Opis:					
Lista obiektów, które chroni lista					
Nazwa obiektu	Rodzaj obiektu	Biblioteka obiektu	Nazwa obiektu	Rodzaj obiektu	Biblioteka obiektu
Lista grup i użytkowników, którzy mają dostęp do listy					
Grupa lub użytkownik	Dozwolony rodzaj dostępu	Zarządzanie listą?	Grupa lub użytkownik	Dozwolony rodzaj dostępu	Zarządzanie listą?

Formularz ochrony kolejki wyjściowej drukarki i stacji roboczej

Tabela 75. Formularz ochrony kolejki wyjściowej drukarki i stacji roboczej

Formularz ochrony kolejki wyjściowej drukarki i stacji roboczej	
Przygotowany przez:	Data:
Instrukcje • Instrukcje dotyczące tego formularza zawiera sekcja ″Zabezpieczanie zbiorów wydruków.″ • Na tym formularzu należy zapisać wszystkie stacje robocze lub kolejki wyjściowe, które wymagają specjalnego zabezpieczenia. • Informacje dotyczące wprowadzania danych z tego formularza zawiera sekcja ″Zabezpieczanie stacji roboczych.″	
Lista parametrów dla ograniczonych kolejek wyjściowych:	

Tabela 75. Formularz ochrony kolejki wyjściowej drukarki i stacji roboczej (kontynuacja)

Nazwa kolejki wyjściowej	Biblioteka kolejki wyjściowej	Wyświetlenie dowolnego zbioru (Display any file - DSPDTA)	Uprawnienia do sprawdzania (Authority to check - AUTCHK)	Sterowane przez operatora (Operator control - OPRCTL)
Stacje robocze szefa ochrony: Jeśli szef ochrony ma ograniczony dostęp do określonych stacji roboczych (wartość systemowa QLMTSECOFR ustawiona jest na tak), poniżej należy wymienić stacje robocze autoryzowane dla szefa ochrony oraz dla wszystkich użytkowników z uprawnieniami *ALLOBJ:				
Poniżej należy wymienić uprawnienia dla ograniczonych stacji roboczych:				
Nazwa stacji roboczej	Grupy lub użytkownicy, którzy są autoryzowani (uprawnienia *CHANGE)			
Uwaga: Ograniczone stacje robocze powinny mieć uprawnienia specjalne *EXCLUDE.				

Formularz instalowania aplikacji

Tabela 76. Formularz instalowania aplikacji

Formularz instalowania aplikacji		Część 1 z 2
Przygotowany przez:		Data:
Instrukcje • Instrukcje dotyczące tego formularza zawiera sekcja ″Planowanie instalowania aplikacji.″ • Dla każdej aplikacji, która ma być zainstalowana, należy przygotować jeden formularz. • Za pomocą formularza należy zaplanować, w jaki sposób ustanowić prawa własności i uprawnienia publiczne dla aplikacji, po ich załadowaniu. • Informacje dotyczące wprowadzania danych z tego formularza zawiera sekcja ″Konfigurowanie ochrony zasobów.″		
Nazwa aplikacji:		
Opis:		
Lista i wyjaśnienie, dlaczego potrzebne są wszystkie profile, które trzeba utworzyć do zainstalowania aplikacji:		
Nazwa biblioteki:		
	Przed zainstalowaniem	Po zainstalowaniu
Właściciel biblioteki		
Właściciel obiektu		
Uprawnienia publiczne do biblioteki		
Uprawnienia publiczne dla obiektu		
Uprawnienia publiczne dla nowych obiektów		
Nazwa biblioteki:		
	Przed zainstalowaniem	Po zainstalowaniu
Właściciel biblioteki		
Właściciel obiektu		

Tabela 76. Formularz instalowania aplikacji (kontynuacja)

Uprawnienia publiczne do biblioteki		
Uprawnienia publiczne dla obiektu		
Uprawnienia publiczne dla nowych obiektów		

Formularz instalowania aplikacji		Część 2 z 2
Nazwa biblioteki:		
	Przed zainstalowaniem	Po zainstalowaniu
Właściciel biblioteki		
Właściciel obiektu		
Uprawnienia publiczne do biblioteki		
Uprawnienia publiczne dla obiektu		
Uprawnienia publiczne dla nowych obiektów		
Nazwa biblioteki:		
	Przed zainstalowaniem	Po zainstalowaniu
Właściciel biblioteki		
Właściciel obiektu		
Uprawnienia publiczne do biblioteki		
Uprawnienia publiczne dla obiektu		
Uprawnienia publiczne dla nowych obiektów		
Nazwa biblioteki:		
	Przed zainstalowaniem	Po zainstalowaniu
Właściciel biblioteki		
Właściciel obiektu		
Uprawnienia publiczne do biblioteki		
Uprawnienia publiczne dla obiektu		
Uprawnienia publiczne dla nowych obiektów		

Dodatek. Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji, omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi, pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie tej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
USA

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

IBM
World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106, Japonia

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego: INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W TAKIM STANIE, W JAKIM SIĘ OBECNIE ZNAJDUJE (“AS IS”) BEZ JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ANI TEŻ GWARANCJI, ŻE PUBLIKACJA TA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych i domniemanych w odniesieniu od pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkownika i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

Informacje na temat możliwości stosowania tego programu, takie jak: (i) wymiana informacji między niezależnie tworzonymi programami a innymi programami (włącznie z tym programem) czy (ii) wspólne używanie wymienianych informacji, można uzyskać pod adresem:

IBM

Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
USA

Informacje takie mogą zostać udostępnione na określonych warunkach, co w niektórych przypadkach może oznaczać opłatę.

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjne IBM na Program lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Niniejsza informacja służy jedynie do celów planowania. Informacja ta podlega zmianom do chwili, gdy produkty, których ona dotyczy, staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance oraz WordPro są znakami towarowymi International Business Machines Corporation oraz Lotus Development Corporation w Stanach Zjednoczonych i/lub w innych krajach.

C-bus jest znakiem towarowym Corollary, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

ActionMedia, LANDesk, MMX, Pentium oraz ProShare są znakami towarowymi lub zastrzeżonymi znakami towarowymi Intel Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

SET oraz logo SET są znakami towarowymi, będącymi własnością SET Secure Electronic Transaction LLC.

Java i wszystkie znaki towarowe dotyczące języka Java są znakami towarowymi Sun Microsystems, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

UNIX jest zastrzeżonym znakiem towarowym Open Group w Stanach Zjednoczonych i w innych krajach.

Nazwy innych przedsiębiorstw, produktów i usług mogą być znakami towarowymi lub znakami usług innych podmiotów.

Warunki pobierania i drukowania publikacji

Zezwolenie na korzystanie z publikacji, które Użytkownik zamierza pobrać, jest przyznawane na poniższych warunkach. Warunki te wymagają akceptacji Użytkownika.

Użytek osobisty: Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

Użytek służbowy: Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich części prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania w każdej sytuacji zezwolenia przyznanego w niniejszym dokumencie, gdy, według uznania IBM, korzystanie z tych informacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych. IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ (″AS IS″) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ CZY PRZYDATNOŚCI DO OKREŚLONEGO CELU.

Wszelkie materiały są chronione prawem autorskim IBM Corporation.

Pobieranie lub drukowanie publikacji z tego serwisu oznacza zgodę na warunki zawarte w niniejszym dokumencie.