УДК 004.9

СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА В ИНТЕРЕСАХ ПОВЫШЕНИЯ УРОВНЯ АВТОМАТИЗАЦИИ ПРОЦЕССОВ УПРАВЛЕНИЯ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИМИ СИСТЕМАМИ

Галанкин А.В., Гончаров А.М., Чащин С.В.

ВКА имени А.Ф. Можайского, Санкт-Петербург, e-mail: Biruk98@gmail.com, Sonpo123@mail.ru

В современных условиях важное значение имеют различные аспекты действенного управления. Актуальность данного материала обусловлена необходимостью автоматизации управления организационно-техническими системами при помощи специального программного обеспечения (СПО). Обозначенное СПО рассматривается как одна из составляющих автоматизированных систем управления, а именно, как система инициализации функций разграничения доступа к ресурсам автоматизированного рабочего места (АРМ) и средствам безопасности общего программного обеспечения, анализа и настройки характеристик АРМ. В целях разработки корректной структуры подобной системы раскрываются основные понятия, реализуемые в общем случае функции и набор требований к системе разграничения доступа. Особое внимание уделяется специальному программному обеспечению, необходимому для разработки системы разграничения доступа к ресурсам АРМ с учетом изложенных требований, а также предлагается модульный вариант ее состава.

Ключевые слова: автоматизированные системы управления, система разграничения доступа, автоматизация процессов управления организационно-техническими системами

IMPROVING INFORMATION TECHNOLOGY ACCESS DIFFERENTIATION TO RESOURCES OF THE WORKSTATION IN ORDER TO IMPROVE THE LEVEL OF AUTOMATION OF MANAGEMENT PROCESSES OF ORGANIZATIONAL-TECHNICAL SYSTEMS

Galankin A.V., Goncharov A.M., Chaschin S.V.

Military Space Academy, St. Petersburg, e-mail: Biruk98@gmail.com, Sonpo123@mail.ru

In modern conditions the importance of various aspects of effective management. The relevance of this material due to automation of management of organizational and technical systems with the help of special software (SSW). Designated SSW is regarded as one of the components of automated control systems, and, namely, as a system initialization functions of controlling access to resources of the automated workplace (AWP) and common security software, analyze and tune the characteristics of the AWP. In order to develop a proper structure of such a system describes the basic concepts implemented in the General case the function and the set of requirements to the system of differentiation of access. Special attention is paid to the special software needed to develop a system of differentiation of access to resources AWP subject to the requirements, and proposes a modular variant of its composition.

Keywords: automated control systems, the system of differentiation of access, automation of management processes of organizational-technical systems

В соответствии с содержанием управленческой деятельности, процесс управления организационно-техническими системами (ОТС) в общем случае складывается из последовательной реализации комплекса ряда взаимосвязанных этапов. Эти этапы составляют цикл управления, который охватывает комплекс мероприятий, выполняемых командирами и органами управления с учетом конкретных условий обстановки. Таким образом, основная цель автоматизации управления ОТС это приведение уровня управленческой деятельности должностных лиц органов управления и самих органов управления в соответствие предъявляемым требованиям за счет широкого использования современных математических методов, информационных технологий, комплексов средств автоматизации (КСА) и эффективных средств систем телекоммуникации [1].

Вопросы выявления, формализации и практической реализации в автоматизированном (автоматическом) режиме циклов управления являются одними из самых сложных в процессе создания автоматизированных систем управления (АСУ) ОТС. Прежде всего, это определяется существенным разнообразием принимаемых должностными лицами решений. В частности, каждый цикл управления ОТС слагается из следующих этапов [1]:

1. Сбор и обработка информации о внешней среде, своих силах и средствах, средствах управления и связи, окружающей обстановке.
2. Уяснение задачи управления и оценки обстановки.

3. Планирование применения ОТС в условиях изменившейся обстановки.

4. Выработка и принятие решения по управлению ОТС.

5. Формирование управляющих воздействий.

6. Доведение управляющих воздействий до подчиненных.

7. Контроль доведения и исполнения распоряжений.

Каждый из перечисленных выше этапов имеет свое содержание, целенаправленность, логику; может выполняться тем или иным методом в зависимости от конкретных условий обстановки и других факторов, а также имеет свои подходы по их автоматизации.

В соответствии с ГОСТ 34.003.90 «Автоматизированные системы. Термины и определения» в зависимости от вида управляемого объекта (процесса) АСУ делят на АСУ технологическими процессами, АСУ предприятиями и АСУ специального назначения. Одним из представителей АСУ специального назначения является АСУ ОТС, которая представляет собой совокупность персонала, КСА и средств телекоммуникаций, реализующую информационную технологию выполнения задач по обработке информации и управлению в интересах эффективного функционирования управляемых объектов.

В настоящее время под АСУ ОТС понимается совокупность информационно-взаимосвязанных органов и объектов управления с их персоналом и техническими средствами, реализующими выработанные наукой и принятые в практике функции и методы управления ОТС в интересах эффективного выполнения боевых задач. Из определений следует, что в АСУ ОТС в целом можно выделить три основные части [1]:

1. Персонал органов и объектов управления.

2. Технические и программные средства управления (КСА).

3. Методы и способы управления, реализуемые персоналом и средствами автоматизированного управления ОТС.

Рассмотрим особенности применения программного обеспечения КСА. Предназначение большинства информационных систем, как специального программного обеспечения, подразумевает хранение и использование больших объемов информации, а также доступ к ним определенного круга лиц [5]. В то же время разграничение доступа к функциям системы и защита от несанкционированного доступа хранящихся в ней данных являются одними из важнейших задач при функционировании обозначенной системы.

В данной статье в качестве информационной системы рассматривается операционная система (ОС), как часть общего программного обеспечения КСА. Одной из особенностей автоматизации процессов управления ОТС является применение различных типов операционных систем, в том числе и иностранной разработки, что обуславливает необходимость использования кроссплатформенных программных средств.

Согласно [4] обеспечение защиты, в том числе КСА, осуществляется:

– системой разграничения доступа (СРД) субъектов к объектам доступа;

– обеспечивающими средствами для СРД.

Система разграничения доступа – это совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах [3].

Основными функциями СРД являются [4]:

– реализация правил разграничения доступа субъектов и их процессов к данным;

– реализация правил разграничения доступа субъектов и их процессов к устройствам создания твердых копий;

– изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;

– управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа;

– реализация правил обмена данными между субъектами для АС и средств вычислительной техники, построенных по сетевым принципам.

Способы реализации СРД зависят от конкретных особенностей средств вычислительной техники и АС. Возможно применение следующих способов защиты и любых их сочетаний [4]:

– распределенная СРД и СРД, локализованная в программно-техническом комплексе (ядро защиты);

– СРД в рамках операционной системы, СУБД или прикладных программ;

– СРД в средствах реализации сетевых взаимодействий или на уровне приложений;

– использование криптографических преобразований или методов непосредственного контроля доступа;

– программная и (или) техническая реализация СРД.

Рассмотрим особенности применения второго способа реализации СРД. Недостатком встроенной СРД является то, что пользователи практически никогда напрямую с ней не общаются, то есть ее закрытость, которая, с одной стороны, предохраняет ее от вмешательства неопытных пользователей, с другой

стороны, по причине неочевидности возможностей СРД даже администраторы операционных систем не в полной мере используют ее потенциал, в некоторых случаях предпочитая инсталлировать специальное программное обеспечение разграничения доступа, которое или дублирует функции СРД ОС или исполняет их при помощи своего интерфейса, используя функции разграничения доступа самой ОС, но при этом ведя свои журналы, предлагая универсальный, с точки зрения разработчика, набор дополнительных возможностей и замедляя работу системы.

Одним из путей разрешения несоответствия существующего программного обеспечения требованиям по применению кроссплатформенного программного средства, позволяющего осуществлять разграничение доступа к ресурсам автоматизированного рабочего места и средствам безопасности общего программного обеспечения, анализ и настройку характеристик АРМ, основанных на ОС, таких как Windows v. 5, 6 и Linux-подобная операционная система МСВС 3.0, является разработка соответствующей системы инициализации функций (СИФ). Такая система позволит с учетом особенностей различных семейств ОС автоматизировать доступ к вышеобозначенным функциям, повысить оперативность типовых действий администратора системы с целью повышения уровня автоматизации процессов управления ОТС.

Исходя из вышесказанного, сформулируем требования к СИФ:

– кроссплатформенность;

– понятный для рядового пользователя интерфейс;

– реализация доступа как к графическим приложениям ОС, так и к консольным, при этом необходимо предусмотреть наиболее часто применяющиеся наборы ключей консольных приложений;

– наличие у СИФ собственного механизма аутентификации, а при большом количестве – администраторов и авторизации, а также журнала осуществленных операций.

Для выполнения требования кроссплатформенности в качестве средства разработки был выбран Qt Creator с набором библиотек Qt версии 4.0 для ОС МСВС 3.0 и Qt версии 4.7 для ОС Windows v. 5, 6.

Qt – кросс-платформенный инструментарий разработки программного обеспечения на языке программирования C++. Отличительная особенность Qt от других библиотек – использование предварительной системы обработки исходного кода для последующей компиляции любым стандартным C++ компилятором, что позволяет во много раз увеличить мощь библиотек, вводя такие понятия, как слоты и сигналы. Qt включает в себя все основные классы, которые могут потребоваться при разработке специального программного обеспечения, начиная от элементов графического интерфейса и заканчивая классами для работы с сетью, базами данных и XML. Qt является полностью объектно ориентированным, легко расширяемым и поддерживающим технику компонентного программирования. Qt Creator включает в себя редактор кода, справку, графические средства Qt Designer и возможность отладки приложений. Qt Creator может использовать GCC или Microsoft VC++ в качестве компилятора и GDB в качестве отладчика.

Для выполнения требования наличия у СИФ собственного механизма аутентификации (авторизации) предлагается включить в ее состав модуль аутентификации (авторизации), включающий в свой состав следующие блоки:

– интерфейс аутентификации (авторизации);

– блок, реализующий механизм аутентификации (авторизации);

– базу данных шифрованных паролей;

– журнал событий.

Модуль авторизации в случае положительного результата прохождения пользователем аутентификации должен после выполнения правил разграничения доступа предоставлять для работы интерфейс главной экранной формы программного модуля СИФ, при этом модулем авторизации должна выполняться фиксация записи о входе каждого пользователя в базу данных, входящую в разрабатываемую систему в качестве отдельного файла. Пароли в базе данных должны храниться в виде хэш-кода шифрования md5.

Для выполнения требования, понятного для рядового пользователя интерфейса, необходимо при его разработке учесть ряд особенностей:

– интерфейс должен быть максимально единообразен для СИФ в различных семействах ОС;

– минимизировать количество экранных форм (ЭФ) СИФ, например, ЭФ аутентификации (авторизации), главная ЭФ с меню и справочной системой, ЭФ выбора необходимых функций;

– максимальное единообразное наименований функций разграничения доступа АРМ, настройки средств безопасности общего программного обеспечения, анализа и настройки характеристик АРМ в различных семействах ОС.

Для организации взаимодействия интерфейса пользователя (администратора) СИФ и ОС МСВС 3.0 предлагается использовать встроенные библиотеки Qt, которые распро-

страняются вместе с самим дистрибутивом ОС. Для организации взаимодействия интерфейса пользователя СИФ и ОС семейства Windows предлагается использовать статические библиотеки Qt, которые будут включены в программной модуль СИФ. Такой подход к применению библиотек Qt наиболее целесообразен для распространения СИФ на различные семейства ОС по причине отсутствия необходимости устанавливать и дополнительное программное обеспечение, и саму СИФ, которую можно будет распространять копированием. Для организации работы модуля программных средств командной строки СИФ обращается к командному интерпретатору ОС, в котором будет функционировать СИФ. Для организации работы модуля программных средств графического интерфейса СИФ в ОС МСВС 3.0 предлагается использовать окружение рабочего стола ELC, а в ОС семейства Windows – диспетчер окон рабочего стола [2].

Для выполнения последнего требования к СИФ рассмотрим отдельно модули программных средств командной строки и графического интерфейса ОС МСВС 3.0 и ОС Windows v. 5, 6.

Предлагаемый состав модуля программных средств командной строки ОС МСВС 3.0:

– консоль elc-term;
– X-терминал для KDE;
– файловый менеджер;
– блок визуализации (БВ) состояния сетевых параметров;
– БВ состояния сетевых портов;
– БВ состояния таблицы маршрутизации;
– БВ информации о системе.

Предлагаемый состав модуля программных средств графического интерфейса ОС МСВС 3.0, предоставляющий доступ к графическим приложениям разграничения доступа к ресурсам АРМ, средствам безопасности ОС и вспомогательной информации:

– блок категорий и уровней секретности;
– блок настройки регистрации событий;
– БВ событий аудита;
– БВ состояния сетевых параметров;
– блок настройки сети;
– блок управления пользователями;
– файловый менеджер.

Качественным отличием СИФ ОС Windows v. 5, 6 является наличие дополнительного модуля, включенного в СИФ, статически линкованных библиотек Qt v. 5.3, что является необходимым условием при распространении системы на АРМ без предустановки библиотек Qt и дополнительного программного обеспечения.

Предлагаемый состав модуля программных средств командной строки ОС Windows v. 5, 6:

– интерпретатор команд ОС Windows;
– БВ анализа сетевых портов;
– БВ состава и состояния сетевого окружения;
– БВ настройки сетевых параметров;
– БВ состояния таблицы маршрутизации;
– БВ информации о системе.

Предлагаемый состав модуля программных средств графического интерфейса ОС Windows v. 5, 6:

– графическая консоль;
– блок управления компьютером;
– групповая политика безопасности;
– локальная политика безопасности;
– БВ журнала событий;
– БВ состояния служб ОС;
– диспетчер устройств;
– межсетевой экран Windows;
– блок управление учетными записями;
– БВ конфигурации системы;
– БВ состава и состояния общих папок и текущих сеансов.

Состав модулей должен обладать возможностью варьироваться в соответствии со специализацией СИФ или требований администраторов системы.

Таким образом, при выполнении требований к СИФ и реализации модулей аутентификации (авторизации), программных средств командной строки, программных средств графического интерфейса различных семейств ОС в должном объеме полученная система позволит автоматизировать доступ к функциям разграничения доступа АРМ и средствам безопасности общего программного обеспечения, анализа и настройки характеристик АРМ, повысить оперативность типовых действий администратора системы, что в конечном итоге дает возможность повысить уровень автоматизации процессов управления ОТС.

Список литературы

1. Волков В.Ф., Галанкин А.В., Федер А.Л. Общая характеристика процесса автоматизированного управления сложными организационно-техническими системами специального назначения Воздушно-космических сил / В.Ф. Волков, А.В. Галанкин, А.Л. Федер // Наукоемкие технологии в космических исследованиях Земли. – 2015. – Т. 7, № 6. – С. 50–54.

2. Галанкин А.В., Гуляев А.Ю., Федер А.Л., Чащин С.В. Структура системы разграничения доступа к ресурсам АРМ и средствам безопасности операционной системы МСВС 3.0 и операционных систем Windows v. 5, 6 / А.В. Галанкин, А.Ю. Гуляев, А.Л. Федер, С.В. Чащин // Теоретические и прикладные проблемы развития и совершенствования автоматизированных систем управления военного назначения. Сборник трудов Всероссийской научно-технической конференции. – 2014. – Ч. 1. – С. 139–142.

3. Руководящий документ ФСТЭК. Защита от несанкционированного доступа к информации. Термины и определения. – М., 1992.

4. Руководящий документ ФСТЭК. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – М., 1992.

5. Федоров А.В., Пьянков В.М., Вихлянцев П.С. Система разграничения доступа к данным на уровне записей и ячеек / А.В. Федоров, В.М. Пьянков, П.С. Вихлянцев // Защита информации. INSIDE. – 2011. – № 3. – С. 2–4.