УДК 004.7

# ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ПРОГРАММНОГО КОМПЛЕКСА АДАПТИВНОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ КОРПОРАТИВНОЙ СЕТИ

**О.М. Демиденко, В.Д. Левчук, А.И. Кучеров**

*Гомельский государственный университет им. Ф. Скорины, Гомель*

# FUNCTIONAL CAPABILITIES OF PROGRAM TOOLS FOR THE ADAPTIVE IDENTIFICATION OF THE CORPORATE NETWORK USERS

**O.M. Demidenko, V.D. Liauchuk, A.I. Kucharau**

*F. Scorina Gomel State University, Gomel*

В статье предложен адаптивный способ защиты вычислительной техники от несанкционированного использования. Приводится оригинальная схема реализации программного комплекса. Рассматриваются преимущества создания и внедрения разработанного программного комплекса.

***Ключевые слова**: авторизация, идентификация, аутентификация, программный комплекс, корпоративная сеть.*

The authors propose an adaptive way of protecting computers from unauthorized use. The original scheme of the software implementation is discussed. The advantages of creating and implementing of program tools are considered.

***Keywords**: authorization, identification, authentication, software system, the corporate network.*

## *Введение*

Практически каждый офисный сотрудник в своей повседневной производственной деятельности в течение всего рабочего дня использует компьютерную технику и коммуникационное оборудование. В настоящее время огромное количество оборудования объединяется в сетевые структуры различных стандартов и типов. Будь то локальные, корпоративные, городские или глобальные сети.

В процессе своей деятельности человек – пользователь, использует различные сетевые ресурсы и в свою очередь создает различные компьютерные продукты: документы, чертежи, программы, мультимедиа и др. Каждый сетевой ресурс и программный продукт является собственностью определенного человека или группы лиц и в конечном итоге может быть собственностью предприятия. Поэтому возникает необходимость обеспечения сохранности создаваемых программных продуктов. Для этих целей используется превеликое множество программных и аппаратных решений. Но основной и первоначальной задачей является обеспечение достоверной идентификации пользователя. Для этих целей операционная система предоставляет большие возможности, но их не достаточно, так как они широко известны злоумышленнику [3], [4]. Поэтому задачи идентификации и аутентификации пользователей корпоративной компьютерной сети являются актуальными.

## *1 Традиционная схема защиты сетевых ресурсов от несанкционированного использования*

Каждый пользователь или группа пользователей в операционной системе обладают определенными правами. Действия, которые пользователь может выполнять в операционной системе, строго определены и описаны. В общем случае возможностей у пользователя много. Он может выполнять большое количество различных операций, на которые может иметь или не иметь права. Эти операции связаны как с работой на локальном компьютере, так с работой в сетевой среде.

Чем выше привилегии пользователя, тем выше у него права и соответственно возможности. Всеми правами в операционной системе обладают только администраторы системы. Для управления правами пользователей в операционной системе в настройках имеется возможность администрирования, где можно назначить права пользователя [2], [5].

Пользователь может выполнять большое количество действий. Но не все из них пользователь имеет право и должен выполнять. А информация может быть как общего, личного, так и служебного использования.

Для повышения дисциплины руководство организаций и предприятий должно иметь возможность управлять правами пользователей локальной вычислительной сети и следить за выполнением их служебных обязанностей.

Обеспечить эти возможности предназначено как встроенное в операционную систему, так и другое системное программное обеспечение.

Современные операционные системы от версии к версии совершенствуют системы, отвечающие за безопасность. Войти в операционную систему возможно только зарегистрированному пользователю. Он должен знать зарегистрированное имя пользователя и его пароль. Если компьютер подключен к компьютерной сети с доменами в качестве рабочей станции, то операционная система потребует помимо имени и пароля, еще и имя домена. Только при совпадении этих трех составляющих пользователю будет разрешен вход в систему. То есть пользователь пройдет аутентификацию [3].

Аутентификация – это установление подлинности личности. Она может быть выполнена при использовании трех вещей: того, что вы знаете, того, что вы имеете, или того, кем вы являетесь. Исторически для идентификации личности в компьютерных системах применяются пароли. Но надеяться на пароли особо не следует. Пароль можно угадать, либо пользователь где-то запишет его, и пароль узнают все. Пользователь также может передать свой пароль другому лицу по какой либо просьбе или с преступным умыслом.

На рисунке 1 показана упрощенная традиционная схема защиты вычислительной техники от несанкционированного использования.

На рисунке 1 видно, что защита сетевых ресурсов от несанкционированного использования слагается из трех составляющих: административные средства, программные средства, аппаратные средства. Административные средства описывают служебные обязанности каждого работника, правила внутреннего распорядка и правила использования вычислительной техники. Административные средства предписывают настройки программных и аппаратных средств. Аппаратные средства чаще всего настраиваются посредствам программных средств, которые в свою очередь состоят из операционной системы, утилит от производителя операционной системы, утилит сторонних производителей, собственные программные разработки. Но и все программные и аппаратные средства имеют свои ограничения, что вносит свои коррективы в административные средства.

Для обеспечения эффективной безопасности вычислительной системы необходимо использовать все три выше описанные составляющие. Но внедрение самых эффективных систем защиты вычислительной техники от несанкционированного использования может обойтись очень дорого, но это еще не значит, что у предприятия будут все необходимые возможности по управлению политикой безопасности. Поэтому многие субъекты стремятся создавать собственные программные комплексы для обеспечения защиты от несанкционированного использования вычислительной техники. При этом программным путем можно следить за всеми действиями пользователя вычислительной системы.

### *2 Адаптивная схема защиты сетевых ресурсов от несанкционированного использования*

Можно предложить следующую схему реализации программного комплекса защиты сетевых ресурсов от несанкционированного использования, которая будет состоять из трех связанных друг с другом программных продуктов. Первый программный продукт будет функционировать на локальной станции. Его главным предназначением будет мониторинг работы пользователя с сохранением результата в файл.


Рисунок 1 – Защита вычислительной техники от несанкционированного использования

Второй программный продукт будет функционировать на сервере безопасности и заниматься сбором и анализом результатов мониторинга активности пользователей на рабочих станциях. Из этих данных можно получить информацию различного рода. Например, сколько пользователь проводит времени за компьютером и какие приложения запускает, какие устройства ввода являются предпочтительными, какие приложения постоянно находятся в оперативной памяти, какой файловый менеджер загружается по умолчанию и т. д. По этим и другим данным можно составить индивидуальный портрет поведения пользователя за компьютером [1].

Третий программный продукт будет заниматься дополнительной идентификацией личности пользователя по хранящемуся на сервере портрету поведения пользователя и по некоторым другим данным. На рисунке 2 показана адаптивная схема программного комплекса по защите сетевых ресурсов.

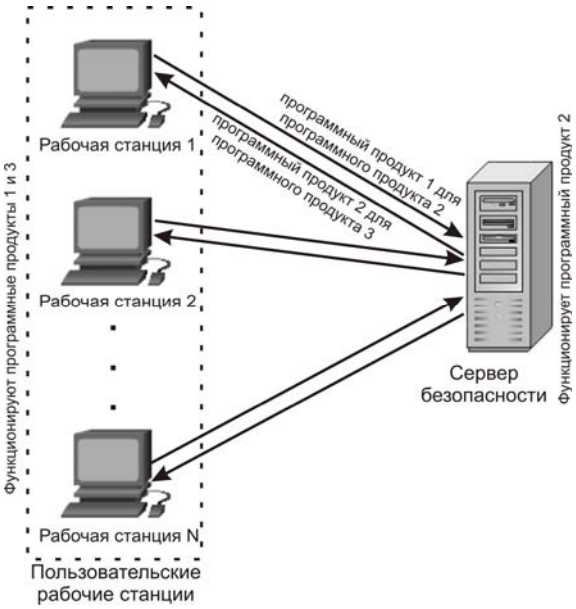


Рисунок 2 – Адаптивная схема программного комплекса мониторинга активности Пользователей

Различие в операционных системах, установленных на рабочих станциях влечет за собой разработку различных версий первого и третьего программных продуктов. Но сервер безопасности должен иметь общий стандартный интерфейс для всех версий.

При использовании в сети технологии «тонкий клиент» все становится еще проще, поскольку достаточно собирать данные в пределах сервера, обслуживающего клиентские рабочие станции (рисунок 3). Функции сервера обслуживания и сервера безопасности можно совместить на одной аппаратной базе. Тогда весь программный комплекс, состоящий из трех программных продуктов, будет работать на одном сервере.

В результате при использовании широко известных средств защиты от несанкционированного использования вычислительной техники совместно с предложенным программным комплексом можно надеяться, что защита будет гораздо более эффективной. При этом предложенный программный комплекс решает, помимо дополнительной защиты от несанкционированного использования вычислительной техники, еще и ряд других задач. Во-первых можно проанализировать, сколько времени каждый пользователь проводит за вычислительной техникой. Во-вторых, можно выяснить какие приложения запускал пользователь и, исходя из этого оценить, сколько времени пользователь решал производственные задачи и сколько находился в состоянии таймаута. В-третьих, анализируя данные на сервере, можно увидеть продолжительность работы каждой рабочей станции от момента включения до момента выключения. Из этого времени элементарно выделяется время простоя вычислительной техники. При творческом подходе перечень опциональных возможностей системных программных средств не ограничивается приведенными выше режимами функционирования. Таким образом, данный программный комплекс обеспечивает эффективные механизмы администрации по управлению предприятием.


Рисунок 3 – Схема программного комплекса мониторинга активности пользователей для технологии «тонкий клиент».

### *3 Этапы разработки программного комплекса*

На первом этапе разработки программного обеспечения создан программный продукт, позволяющий автоматизировать действия администратора корпоративной сети по регистрации пользователей на контроллере домена. Для

предоставления доступа к ресурсам сети необходимо применять средства операционной системы, которые позволяют разграничить права пользователей на используемые данные. Операционная система является связующим звеном между электронными средствами и пользователем. Вся информация хранится в электронном виде на компьютерах.

Разграничением прав доступа пользователей к различной информации занимается администратор корпоративной сети. Для осуществления своей деятельности ему необходимо обрабатывать большие объемы информации, содержащей сведения о компьютерах и пользователях корпоративной сети. На рисунке 4 представлена схема традиционной работы администратора корпоративной сети.

Для усовершенствования работы администратора сети по разграничению прав доступа пользователей к информационным ресурсам сети используется разработанная авторами автоматизированная система ДОСТУП, которая позволяет уменьшить ошибки, сбои и дублирование служебной информации в работе администратора и операционной системы. На рисунке 5 представлена схема работы администратора сети посредством автоматизированной системы.

Автоматизированной системой реализуются следующие задачи:

– ввод первичной информации в базу данных Active Directory [2];

– модификация, удаление устаревшей информации;

– ввод вторичной информации;

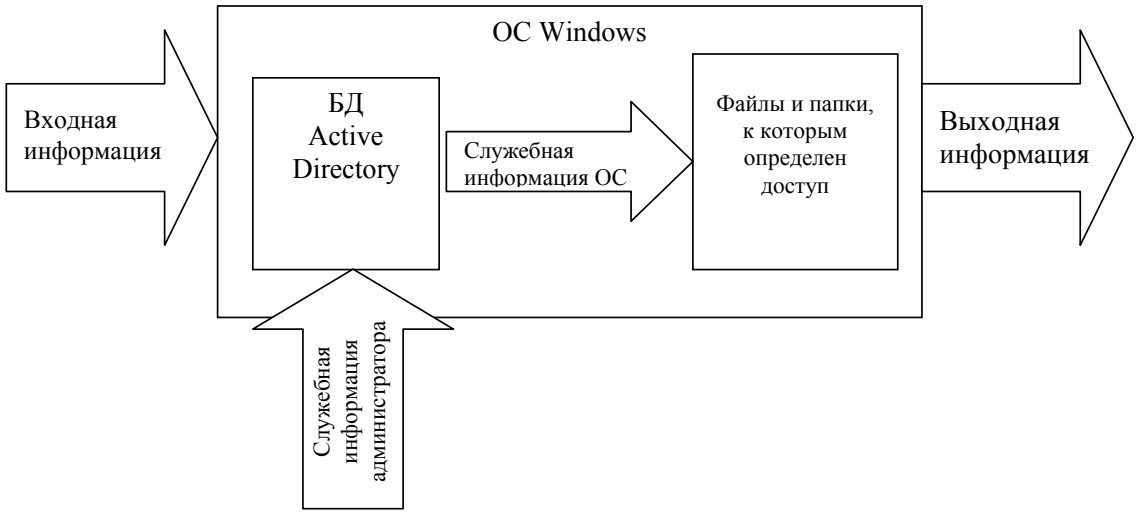


Рисунок 4 – Структура неавтоматизированной работы администратора сети средствами операционной системы

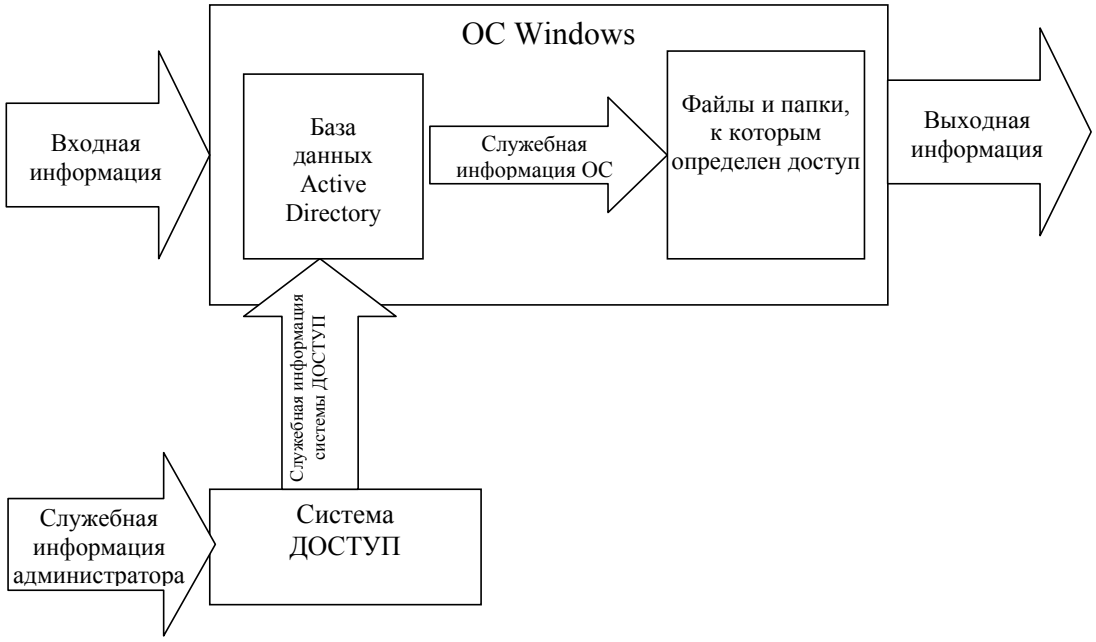


Рисунок 5 – Структура автоматизированной работы администратора сети

– репликация базы данных Active Directory;

– поисковые запросы в базе данных Active Directory;

– вывод результатов поиска по запросам;

– создание личных папок пользователей корпоративной сети;

– разграничение прав доступа к вычислительным ресурсам корпоративной сети;

– ведение аудита входа и выхода на рабочей станции;

– ведение аудита использования сетевых ресурсов;

– автоматизация ввода вторичной информации;

– автоматизация модификации и удаления устаревшей информации.

На втором этапе разработки программного обеспечения создан программный комплекс адаптивной идентификации пользователей корпоративной сети. В его основе находится сбор информации о пользователях на узлах сети и формирование идентификационного портрета каждого пользователя.

В качестве узлов сети приняты персональные компьютеры, соединенные посредством сетевой среды, выполненной по одной из топологий. Рабочая нагрузка на узлах сети состоит из рабочей нагрузки, создаваемой операционной системой, и рабочей нагрузки, создаваемой пользователями вычислительной системы. В процессе функционирования операционной системы на узле сети порождается рабочая нагрузка посредством системных процессов. Кроме этого, пользователь вычислительной системы по роду своей деятельности выполняет различные задачи, которые в операционной системе представляются как пользовательские процессы. Пользователь может использовать следующие программные приложения: офисные пакеты; бухгалтерские пакеты; игры; интернет; графические пакеты и мультимедиа; языки программирования; специализированные программные средства.

Программный комплекс адаптивной идентификации пользователей корпоративной сети архитектурно построен на основе модульного принципа разработки приложений. Каждый модуль выполняет свои определенные функции, что позволяет уменьшить влияние одного программного модуля на другой. Это обеспечивает создание более гибкого и легко расширяемого по функциям программного модуля. Программные модули будут собирать информацию о действиях пользователей, например: скорость набора на клавиатуре (количество символов в единицу времени); скорость нажатий каждой кнопки манипулятора типа «мышь»; запускаемые приложения; время входа в узел сети; время выхода из узла сети; время блокировки пользователем узла сети; время простоя узла сети и т.д.

На основе собранной информации, создается идентификационный портрет пользователя корпоративной сети. Данные портреты пользователей хранятся в базе данных и сравниваются с текущей информацией о пользователе. Если сохраненный идентификационный портрет пользователя существенно не совпадает с текущей информацией о пользователе, то с определенной долей вероятности система адаптивной идентификации пользователей корпоративной сети принимает решение, что на узле сети работает пользователь, выдающий себя за другого пользователя. Методик по определению мнимых пользователей на основе идентификационного портрета пользователя достаточно много, и еще предстоит выяснить наиболее приемлемую из них [1]. Для этих целей необходимо продолжить научные исследования в этой области.

Чем дольше созданный программный комплекс будет функционировать на рабочих станциях в корпоративной сети, тем большими данными будет обладать база данных, в которой будут храниться действия пользователей. И тем более адекватно программный комплекс будет определять пользователя, выдающего себя за другого пользователя корпоративной сети.

Санкции, применяемые к таким нарушителям, определяет администрация организации, которая будет использовать созданный программный комплекс. В настоящее время рассмотренные в данной статье программные средства проходят опытную эксплуатацию.

Как выше отмечалось, из собранной информации можно делать и другие выводы. Например, сколько каждый узел сети работает в течении дня, недели, месяца и т.д. От этого будет зависеть, как часто необходимо проводить профилактические работы с тем или иным узлом. В процессе эксплуатации программного комплекса будут уточняться цели и задачи созданной системы.

ЛИТЕРАТУРА

1. *Деннинг, В.* Диалоговые системы «человек-ЭВМ». Адаптация к требованиям пользователя / В. Деннинг, Г. Эссинг, С. Макс – М. : «Мир», 1984.

2. *Зубанов, Ф.В.* Active Directory: подход профессионала / Ф.В. Зубанов. – М. : Издательско-торговый дом «Русская редакция», 2003.

3. *Палмер М.* Проектирование и внедрение компьютерных сетей: учебный курс / 2-е изд., перераб. и доп.; пер. с англ. / М. Палмер, Р.С. Брюс. – СПб. : БХВ-Петербург, 2004.

4. *Соловьев, В.Н.* Операционные системы / В.Н. Соловьев. – М. : Радио и связь, 1991.

5. *Чен, В.* Реестр Windows NT для профессионалов / Чен Веинг. – СПб. : Питер, 1999.

*Поступила в редакцию 11.07.10.*