Известия Гомельского государственного университета
имени Ф. Скорины, №4(55), Ч2, 2009

УДК 681.3

Предпосылки создания программного комплекса мониторинга активности пользователей

А. И. Кучеров, А. В. Воруев

Различным организациям в процессе функционирования необходимо контролировать работу своих сотрудников. Для этого создают специальные службы и подразделения. В помещениях устанавливают скрытые камеры. Но даже если поставить возле каждого сотрудника по специальному человеку, который будет контролировать его работу, за всеми действиями подопечного невозможно уследить. А еще действуют физиологический и человеческий факторы. Также может быть преступный сговор сотрудника и надзирателя. Это крайнее проявление недружественности работников по отношению к организации.

Намного проще проследить за действиями сотрудников, которые проводят большую часть своего рабочего времени за компьютером. Им также можно ограничить, разрешить или запретить некоторые действия. Для этих целей в современных операционных системах имеются определенные возможности.

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

Аутентификация – это установление подлинности личности. Она может быть выполнена при использовании трех вещей: 1) того, что вы знаете, 2) того, что вы имеете, или 3) того, кем вы являетесь. Исторически для идентификации личности в компьютерных системах применяются пароли. Но надеяться на пароли особо не следует. Пароль можно угадать. Пользователь иногда записывает пароль. Пользователь также может передать свой пароль другому лицу, по какой-либо просьбе или с преступным умыслом.

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. Пользователь может выполнять большое количество различных операций, на которые он может иметь или не иметь прав. Эти операции связаны как с работой на локальном компьютере, так и при работе в локальной вычислительной сети.

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.

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

На рисунке 1 видно, что защита вычислительной техники 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 определенные коррективы в административные средства.

Рисунок 1 – Защита вычислительной техники от несанкционированного использования

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 вас будут все необходимые возможности по управлению политикой безопасности. Поэтому многие организации 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.

Можно предложить следующую схему реализации программного комплекса, которая будет состоять из трех программных продуктов, связанных друг с другом. Первый программный продукт будет функционировать на локальной станции, его главным предназначением будет мониторинг работы пользователя с сохранением результата в файл. 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 и т.д. По этим и другим данным можно составить портрет поведения пользователя. 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 схема программного комплекса.

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 ра-

бочие 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.

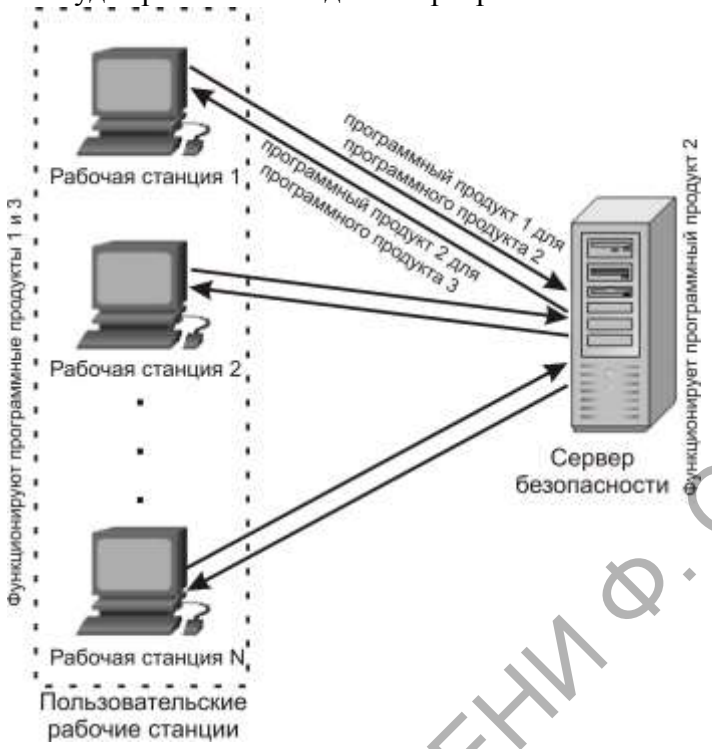

Рисунок 2 – Схема программного комплекса мониторинга активности пользователей.

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

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, определить, сколько времени пользователь работал, а сколько – развлекался. В–третьих, анализируя данные на сервере, можно увидеть продолжительность работы каждой рабочей станции от момента включения до момента выключения. Из этого времени выделить время простоя вычислительной техники. Программный комплекс после разработки даст дополнительные средства администрации по управлению организацией.

Abstract. The probable scheme protection of computer facilities against unauthorized usage is described in the paper. The original scheme of implementation of the program complex is presented. The possible benefit from the creation and implementation of the developed program complex is examined.

Гомельский государственный
университет им. Ф. Скорины

Поступило 15.10.08