УДК 004.4'2

**А. И. Кучеров, Е. А. Левчук, Г. Ю. Дорошкова,
С. В. Дробышевский, С. А. Борсуков**

# ПРЕДПОСЫЛКИ СОЗДАНИЯ ПРОГРАММНОГО КОМПЛЕКСА ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СЕТИ

*Рассматривается проблема идентификации личности пользователей в корпоративных сетях. Здесь рассмотрены плюсы и минусы, которые имеют традиционные методы в сфере защиты компьютерных сетей и приведены аргументы в пользу выгодности создания своего программного комплекса по решению данной проблемы. Описывается вероятная схема защиты вычислительной техники от несанкционированного использования. Приводится оригинальная схема реализации программного комплекса и возможная выгода от его создания и внедрения.*

## Введение

В начале XXI в. в сфере информационно-коммуникационных технологий обозначились новые проблемы.

Темп внедрения компьютерных технологий в экономику достиг рекордных размеров. Создается все больше интернет-магазинов, «виртуальных» филиалов банков, электронных фондовых и валютных бирж. Электронный бизнес перемещается в глобальную сеть Интернет. Сохранить конфиденциальность трансакций и целостность данных становится проблемой. Эта проблема из чисто технической перешла в категорию ключевых проблем бизнеса и по важности сравнялась с разработкой стратегии бизнеса в Интернете.

Тенденция расширения операций купли-продажи в распределенных сетях проявляется достаточно отчетливо и нет предпосылок к смене ее характера в будущем. Специальная литература наполнена прогнозами о сроках, когда все дееспособные члены общества столкнутся с необходимостью применения технологий криптографической защиты информации, безопасностью хранения и уничтожения криптографических ключей. Оппоненты такого направления развития тотальной информатизации общества доказывают отсутствие надежд на переход общества в состояние, когда каждый его член будет корректно выполнять все усложняющиеся операции по защите информации в процессе обеспечения своей жизнедеятельности. Последняя точка зрения послужила катализатором развития технологий по автоматическому распознаванию (идентификации) дееспособных субъектов на основе анализа их биометрических признаков (отпечатков пальцев, структуры ладони и т. д.). Другая проблема: со временем все чаще приходится иметь дело с виртуальным образом человека, с которым не было встреч в реальном пространстве. В традиционном магазине покупатели отличаются по своему внешнему виду, в сети Интернет все выглядят одинаково. В реальной жизни можно выдать себя за другого, в сети Интернет это делается намного проще и без дополнительной проверки нельзя идентифицировать виртуального партнера. Однако если идентификация оказалась успешной, часто этого недостаточно. Для заключения сделки требуются подпись и гарантии ее достоверности.

## Традиционные подходы к решению проблемы

Перечень проблем, решение которых сводится к созданию систем автоматической идентификации личности по ее биометрическим признакам, можно продолжать достаточно долго. Однако пути их решения должны выбираться с учетом состояния экономики в ближайшей перспективе.

Ориентация на массовое применение систем автоматической идентификации личности (человека) приводит к необходимости решать задачу по минимизации их стоимости. В силу текущего экономического состояния все исследования, проводимые в этой области, исключают применение специализированных дорогостоящих устройств. В обобщающих публикациях некоторых ученых по «биометрической идентификации» предлагается вообще отказаться от специализированной аппаратной поддержки и ориентироваться на стандартные устройства ввода информации, придаваемые к ПЭВМ: клавиатуру, звуковую карту, сканер, графический планшет, мышь.

Применяемые на сегодняшний день способы распознавания пользователей ПЭВМ основаны на использовании паролей и (или) специализированных устройств (смарт-карт, «электронных ключей»). Эксплуатация таких систем безопасности выявила их недостатки. Зачастую пароли перехватываются, специализированные устройства похищаются или подделываются. Наблюдаются ситуации, когда один из пользователей сознательно передает свой пароль постороннему лицу. Например, в дистанционном образовании при тестировании студенты готовы заменить себя более осведомленным в изучаемом предмете лицом. Аналогичных примеров из других областей можно привести множество. Таким образом, существуют актуальные задачи как повышения надежности автоматической идентификации зарегистрированных пользователей, так и обнаружения незарегистрированных лиц, которым представилась возможность взаимодействовать с мобильными терминалами распределенных сетей. Требование «Обнаружение чужого» вносит ограничения в выбор подходов для решения этой задачи. В рамках новых технологий идентификации лиц по отпечаткам пальцев, изображению сетчатки глаза и др. не решается проблема скрытности процесса идентификации. Процедуры съема информации настораживают (отпугивают) «чужого» и вызывают неоднозначное отношение у «своих». Выход из подобной ситуации просматривается в использовании для идентификации динамических характеристик человека, к которым относят особенности произношения и написания паролей, ввод их с клавиатуры и др. Во всяком случае, этот путь позволяет реализовать отмеченную выше необходимость избежать применения дорогостоящих (и «настораживающих» идентифицируемого) устройств. Вопрос в другом: достаточную ли информацию дают динамические характеристики, чтобы выйти на приемлемые уровни надежности идентификации лиц.

Налицо следующая ситуация. Есть потребность в системах идентификации личности по динамике формирования подсознательных движений (клавиатурному почерку, особенностям произношения речевых сигналов, динамике написания паролей, тремору двигательных органов). Предлагаемые зарубежные программные продукты дороги, методика оценки их параметров неизвестна и не оговаривается международными стандартами, алгоритмы функционирования известны узкому кругу производителей систем. Поэтому возникла идея о создании собственной системы идентификации личности, которая базировалась бы на системах идентификации, применяемых в современных операционных системах.

## Предпосылки создания программного комплекса

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 и глобальной 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 корпоративной 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 видно, что защита информации 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, из собственных программных разработок. Но и все программные и аппаратные средства имеют свои ограничения, что вносит определенные коррективы в административные средства.


*Рис. 1.* Защита информации от несанкционированного использования

Для обеспечения эффективной безопасности вычислительной системы необходимо использовать все три выше описанные составляющие. Однако 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 корпоративной сети, но это неприемлемо для глобальных сетей.

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 со-

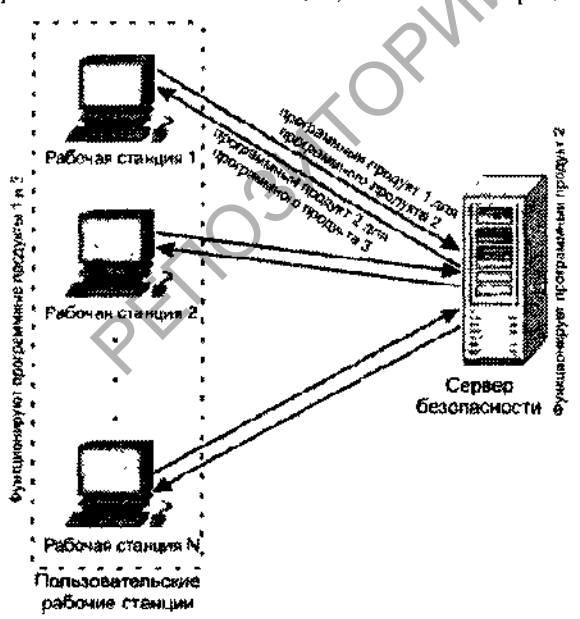


*Рис. 2.* Схема программного комплекса мониторинга активности пользователей

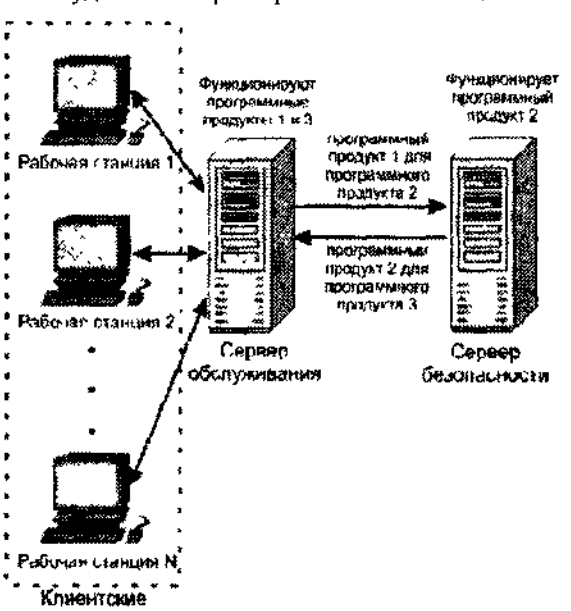


*Рис. 3* Схема программного комплекса мониторинга активности пользователей для технологии «тонкий клиент»

хранением 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. Схема программного комплекса показана на рис. 2.

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 (рис. 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.

## Заключение

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. Может быть, и *в-четвертых* и *в-пятых*, если это потребуется. Программный комплекс после разработки даст дополнительные средства администрации по управлению организацией.

## Литература

*Воруев, А. В.* Удаленный контроль и управление процессами в локальных сетях / А. В. Воруев, О. М. Демиденко, А. И. Кучеров // Известия Гомельского гос. ун-та имени Ф. Скорины. – Гомель. – 2007. - № 5 (44). – С. 98–100.

*Кучеров Александр Иванович, ассистент кафедры автоматизированных систем обработки информации физического факультета Учреждения образования «Гомельский государственный университет имени Франциска Скорины», kucherov@gsu.by*

*Левчук Елена Аркадьевна, доцент кафедры информационно-вычислительных систем УО «Белорусский торгово-экономический университет потребительской кооперации», кандидат технических наук, доцент, lv@gsu.by*

*Дорошкова Галина Юрьевна, преподаватель-стажер кафедры автоматизированных систем обработки информации физического факультета Учреждения образования «Гомельский государственный университет имени Франциска Скорины», gnautova@gsu.by*

*Дробышевский Станислав Витальевич, студент кафедры автоматизированных систем обработки информации физического факультета Учреждения образования «Гомельский государственный университет имени Франциска Скорины».*

*Борсуков Сергей Александрович, студент кафедры автоматизированных систем обработки информации физического факультета Учреждения образования «Гомельский государственный университет имени Франциска Скорины».*