

**КСЗИ «ПАНЦИРЬ-К»  
для ОС Windows  
2000/XP/2003.**

## **КСЗИ «ПАНЦИРЬ-К» ДЛЯ ОС WINDOWS 2000/XP/2003 –**

### **ОПТИМАЛЬНОЕ РЕШЕНИЕ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ**

“...Знание существует для того, чтобы его распространять...”

Эмерсон

Сегодня, наверное, уже нет необходимости убеждать кого-либо в том, что современные ОС, в частности ОС семейства Windows, нуждаются в дополнительной защите. Эту потребность в равной мере ощущают как представители государственных организаций, которым необходимо выполнять требования нормативных документов в области защиты информации, регламентирующих условия обработки конфиденциальной информации и персональных данных, так и представители коммерческих структур, стремящихся к стабильности и защищенности своего бизнеса.

На сегодняшний день можно выделить тенденцию к стремлению решить задачу защиты информации профессионально и в комплексе. При этом помимо необходимости выполнения средствами защиты информации формальных требований, предъявляемых государственными и отраслевыми стандартами, что должно подтверждаться соответствующими сертификатами, для потребителя не менее важно, чтобы эти средства были эффективны, универсальны, максимально просты в использовании, не предъявляли бы дополнительных требований к инфраструктуре организации и, к тому же, были бы недороги. Все это в совокупности и определяет потребительские свойства современного средства защиты.

## Что такое КСЗИ «Панцирь-К» для ОС Windows 2000/XP/2003?

Комплексная система защиты информации (КСЗИ) «Панцирь-К» для ОС Windows 2000/XP/2003 – программный комплекс защиты конфиденциальной информации и персональных данных, предназначенная для защиты, как автономных компьютеров, так и компьютеров в составе сети предприятия.

КСЗИ реализована программно. Одна и та же клиентская часть может устанавливаться на различные ОС семейства Windows (2000/XP/2003). В настоящее время осуществлена доработка КСЗИ «Панцирь-К» для работы с ОС Windows Vista - КСЗИ «Панцирь-К» для ОС Windows 2000/XP/2003/Vista/2008.

Реализованные подходы к построению обеспечивают высокую надежность функционирования КСЗИ и независимость от установленных обновлений (patch-ей) ОС и приложений – основные компоненты КСЗИ – системные драйверы протестированы с использованием соответствующих средств отладки производителя ОС.

Все механизмы защиты реализованы собственными средствами, не использован ни один встроенный в ОС механизм защиты, многие из которых обладают серьезными архитектурными недостатками.

КСЗИ «Панцирь-К» собственными средствами реализует все требования, предъявляемые к защите конфиденциальной информации от несанкционированного доступа. КСЗИ сертифицирована ФСТЭК по **5 классу СВТ** (сертификат №1144, ограничения по использованию в сертификате отсутствуют) и выполняет все требования к классу защищенности **1Г для АС**.

К комплексной системе защиты КСЗИ может быть отнесена, ввиду того, что она служит для эффективного противодействия, как известным, так и потенциально возможным атакам на защищаемые ресурсы, что обеспечивается устранением архитектурных недостатков защиты современных ОС Windows, т.е. позволяет решать задачи защиты информации в общем виде (что невозможно при использовании всевозможных средств контроля).

КСЗИ может применяться для защиты, как от внешних, так и от внутренних ИТ-угроз, обеспечивая эффективное противодействие атакам и со стороны хакеров, и со стороны инсайдеров (санкционированных пользователей, допущенных к обработке информации на защищаемом вычислительном средстве).

КСЗИ также может использоваться для эффективного противодействия вирусным атакам, эксплойтам, вредоносным и шпионским и любым иным деструктивным программам, атакам на ошибки программирования в системном и прикладном ПО; содержит в своем составе, как механизмы защиты от несанкционированного доступа, так и механизмы криптографической защиты данных.

В части криптографической защиты конфиденциальности информации в КСЗИ реализована возможность шифрования данных (на жестком диске и на отчуждаемых накопителях, локальных и разделенных в сети), при этом обеспечивается шифрование «на лету» (прозрачно для пользователя) любого заданного администратором файлового объекта (диска, папки, файла). Реализованная ключевая политика позволяет защитить данные от раскрытия даже при хищении компьютера и при наличии ключа шифрования, позволяет осуществлять коллективный доступ к локальным и разделенным в сети

зашифрованным объектам.

Для шифрования данных в КСЗИ интегрированы возможности использования сертифицированных криптопровайдеров «Signal-COM CSP» и «КриптоПро CSP 3.0 (3.6 для ОС Vista)» (соответствующих требованиям ФСБ РФ к шифрованию конфиденциальной информации по классам «КС1» и «КС2»).

В КСЗИ внедрены инновационные технологии защиты информации (НОУ-ХАУ компании). На способы и технические решения, реализованные в КСЗИ, получено 11 патентов на изобретения. Реализация практически каждого механизма защиты КСЗИ оригинальна (запатентована), обладает принципиально новыми свойствами защиты, что позволяет принципиально поднять уровень ее эффективности и расширить функциональные возможности.

К инновационным технологиям, реализованным в КСЗИ, могут быть отнесены: включение в основные механизмы контроля доступа к ресурсам (к файловым объектам, к реестру ОС, к сетевым ресурсам и т.д.) субъекта «процесс», как самостоятельного субъекта доступа, контроль сервисов олицетворения; разделение между пользователями ресурсов, не разделяемых ОС и приложениями, вероятностный контроль доступа к файловым объектам (мандатный принцип контроля доступа несет в себе угрозу заражения макровирусами конфиденциальных данных), контроль подключения устройств, в том числе, по их серийным номерам и др.

### **КСЗИ «Панцирь-К» предоставляет следующие возможности:**

- Использование аппаратных решений для авторизации пользователей при входе в систему и при доступе к критичным файловым объектам (смарт-карта, Aladdin eToken, ruToken, iButton);
- Разграничения и аудит работы пользователей с локальными и сетевыми ресурсами (файловые ресурсы - FAT/NTFS/DFS/любые монтируемые ФС), ресурсы реестра ОС, сменные носители, принтеры, сервисы олицетворения, буфер обмена и т.д.);
- Разграничения и аудит работы программ (приложений) с локальными и сетевыми ресурсами;
- Разграничения и аудит работы пользователей с устройствами с использованием их серийных номеров (Flash-диски, CD/DVD, USB, WiFi, Bluetooth, IrDA, IEEE1394/ FireWire, PCMCIA, COM/LPT и т.д.);
- Разграничения и аудит работы пользователей и приложений с локальными и глобальными сетями (ЛВС, Internet/Intranet) – персональный Firewall;
- Шифрование данных «на лету» (3DES, AES, DES, ГОСТ 28147-89), включая сетевые ресурсы, скрытие, разграничение доступа, а также гарантированное удаление остаточной информации, реализации коллективного доступа к зашифрованным данным;
- Контроль рабочего времени пользователя, в том числе, средствами компьютерного видео наблюдения;
- И многое другое.

Примеры интерфейсов КСЗИ приведены на рис.1.

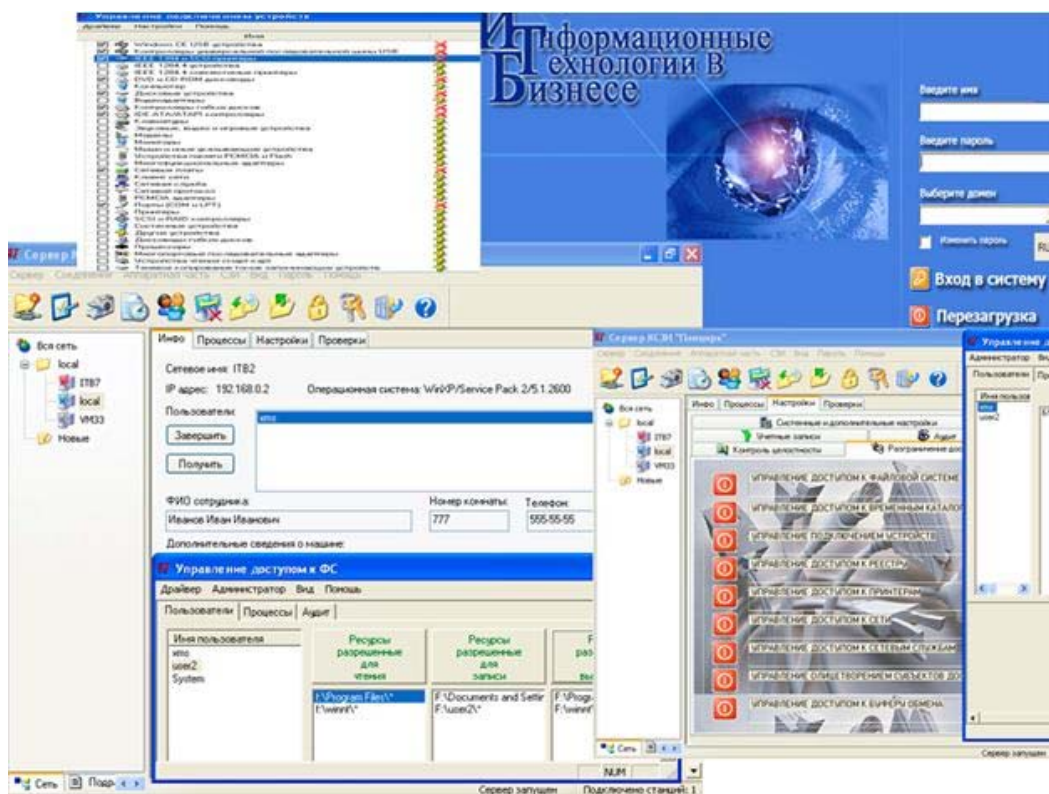


Рис.1. Примеры интерфейсов КСЗИ «Панцирь-К»

## Почему КСЗИ «Панцирь-К» оптимальное решение?

Отличие	Преимущество
<b>КСЗИ – эффективное средство защиты информации</b>	КСЗИ – это Российская разработка, сертифицированная ФСТЭК, создана устранять многочисленные уязвимости в ОС и приложениях в общем виде, в том числе, вызванные архитектурными недостатками ОС
<b>КСЗИ сертифицирована ФСТЭК по 5 классу СВТ</b>	5 класс СВТ – это необходимый (не завышенный) и достаточный класс защищенности, при обработке конфиденциальной информации
<b>Полностью программная реализация</b>	КСЗИ при внедрении и эксплуатации не предъявляет никаких дополнительных системных и аппаратных требований, легко масштабируется, устанавливается, может использоваться на различных аппаратных платформах и гибко настраиваться под нужды организации
<b>Реализация всех требований к АС класса защищенности 1Г собственными средствами</b>	Благодаря выполнению КСЗИ всех требований собственными средствами, для успешной аттестации компьютеров и сетей организации не требуется внедрения каких-либо дополнительных сторонних продуктов

<p><b>Полноценная защита данных от внешних угроз</b></p>	<p>Большой набор механизмов и гибкость их настройки позволяет обеспечить защиту данных от вирусных эпидемий, троянов, деструктивных и шпионских программ, атак на уязвимости ОС и приложений общем виде</p>
<p><b>Полноценная защита данных от инсайдеров</b></p>	<p>Благодаря широкому спектру механизмов контроля доступа к ресурсам и аудита действий пользователей, подсистеме шифрования данных, обеспечивается защита данных от неправомерных действий сотрудников компании</p>
<p><b>Контроль рабочего времени сотрудника</b></p>	<p>Администратор безопасности имеет возможность осуществлять контроль рабочего времени пользователей за любой промежуток времени, возможность визуального контроля действий пользователя при работе с критичными программами и приложениями.</p>
<p><b>Удаленное администрирование и контроль в реальном времени</b></p>	<p>Серверная часть позволяет администратору безопасности со своего рабочего места осуществлять настройку и контроль функционирования системы защиты, а так же пресекать попытки НСД к информации в реальном времени</p>
<p><b>Инновация технических решений</b></p>	<p>На реализацию основополагающих механизмов защиты получено 11 патентов РФ, что подтверждает новизну</p>

	реализованных технических решений
<b>Самая низкая цена среди решений подобного класса</b>	Благодаря отсутствию дорогостоящих аппаратных компонент, сертификации по требуемому для обработки конфиденциальной информации и персональных данных классу защищенности, цены на КСЗИ существенно ниже, чем на аналогичные добавочные средства защиты. Программная реализация позволяет проводить гибкую ценовую политику при увеличении объемов поставки

### **Почему КСЗИ «Панцирь-К» эффективное средство защиты?**

Эффективность средства защиты обуславливается тем, в какой мере им могут решаться ключевые задачи защиты информации, по сути, это является одним из важнейших потребительских свойств средства защиты.

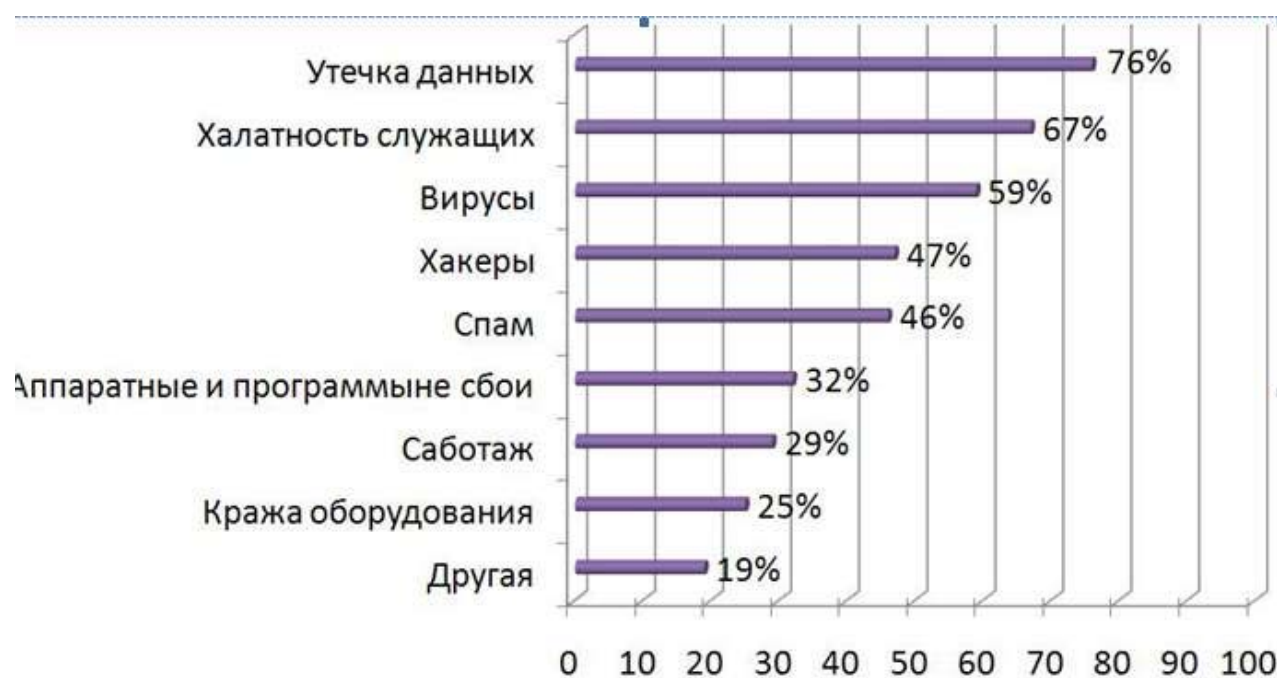
В требованиях нормативных документов в области защиты информации (в соответствии с которыми сертифицируется средство защиты информации) даже теоретически не могут быть определены все актуальные для решения задачи защиты, ввиду того, что средство защиты создается под конкретную платформу (ОС), архитектура которой постоянно (при переходе от версии к версии) видоизменяется, видоизменяются угрозы, уязвимости, как следствие, задачи защиты информации. Претерпевают изменения и информационные технологии, что также вносит дополнительные требования к реализации защиты. Все это обуславливает необходимость создания средства защиты информации,

обеспечивающего не только выполнение требований нормативных документов, но и позволяющего решать насущные задачи защиты информации в АС предприятия, в противном случае, говорить о какой-либо эффективности средства защиты информации не представляется возможным.



Для ответа на вопрос: что и от кого следует защищать в современных условиях обратимся к некоторым исследованиям и к соответствующей статистике.

В части иллюстрации мнения на этот счет потребителей средств защиты весьма показательное исследование, проведенное компанией Perimetrix, один из результатов которого приведен на рис.2.



Данные аналитического центра Perimetrix 2008г.

Рис. 2

Посмотрев внимательно на рис.2, можно сделать вывод о том, что практически в равной мере для потребителей сегодня актуально решение задач защиты, как от внешних, так и от внутренних ИТ-угроз, обеспечение эффективного противодействия атакам и со стороны хакеров, и со стороны инсайдеров

(санкционированных пользователей, допущенных к обработке информации на защищаемом вычислительном средстве), решение задач эффективного противодействия вирусным атакам, эксплойтам, вредоносным, шпионским и любым иным деструктивным программам, атакам на ошибки программирования в системном и прикладном ПО. Другими словами, задачи защиты должны решаться в комплексе.

Прежде, чем переходить к рассмотрению отдельных задач защиты и путей их возможного решения в комплексе, остановимся на первостепенной задаче (по сути, это то, с чего начинается защита) – на задаче формирования объекта защиты.

Актуальность данной задачи обуславливается тем, что, с одной стороны, в настоящее время на практике используются универсальные ОС, одним из основных потребительских свойств которых является универсальность в части возможности использования ПО и иных ресурсов, в первую очередь, устройств. В корпоративных же приложениях (в АС предприятия) требования к подобным средствам диаметрально противоположны – следует использовать только те ресурсы, которые необходимы для решения производственных, либо бизнес задач. С другой стороны, объект, функционал и набор возможных ресурсов для которого не определены (не сформированы средством защиты), защитить невозможно даже теоретически.

## 1. Механизмы формирования объекта защиты.

К механизмам формирования объекта защиты в КСЗИ относятся:

- Механизм обеспечения замкнутости программной среды. В КСЗИ могут задаваться папки (это каталоги Windows (для разрешения запуска системных процессов), Program Files и др.), из которых разрешен запуск программ (в них администратор должен штатными средствами ОС устанавливать приложения), и которые запрещено модифицировать - какая-либо несанкционированная модификация этих папок предотвращается, даже при наличии у злоумышленника системных прав. В итоге, принципиально предотвращается возможность запуска любой деструктивной программы (вируса, трояна, шпионской программы, эксплойта и др.), причем при попытке их запуска, как удаленно, так и локально – инсайдером. Весь компьютер может быть «заражен» подобными программами, но запустить их при этом невозможно. Не требуется какого-либо сигнатурного анализа – задача защиты решается в общем виде без какого-либо влияния на производительность системы – этот механизм защиты, в том числе, является основой антивирусной защиты (позволяет в принципе предотвратить наиболее критичные вирусные атаки, связанные с запуском деструктивной программы). Вообще говоря, без реализации в системе замкнутости программной среды говорить о какой-либо защите не приходится в принципе – если злоумышленник может локально, либо удаленно запустить собственную программу, то, так или иначе, он обойдет любую защиту;
- Механизм управления подключением (монтированием) к системе устройств. Этот механизм призван обеспечить жестко заданный набор устройств, подключение которых разрешается к системе. Только при

реализации подобного механизма можно однозначно описать объект защиты (автономный он или сетевой, с возможностью или без использования отчуждаемых накопителей и каких, и т.д., и т.п.). Важен он и в том смысле, что к устройствам, которые разрешено монтировать к системе, должны разграничиваться права доступа – и без реализации данного механизма потребуется разграничивать доступ ко всем устройствам (что, попросту, глупо). КСЗИ позволяет разрешить монтирование к системе только необходимых для работы пользователя устройств (в отличие от ОС Windows XP, в КСЗИ реализована разрешительная политика управления подключением устройств – это единственно возможное корректное решение задачи защиты), причем с учетом серийных номеров их производителей (например, два Flash-устройства могут быть различимы между собой – монтировать можно разрешить не просто устройства, а конкретные устройства, идентифицируемые их серийными номерами – без подобной возможности системы защиты трудно говорить о реализации каких-либо организационных мер защиты при работе с внешними накопителями).

## 2. Механизмы защиты от инсайдерских атак.

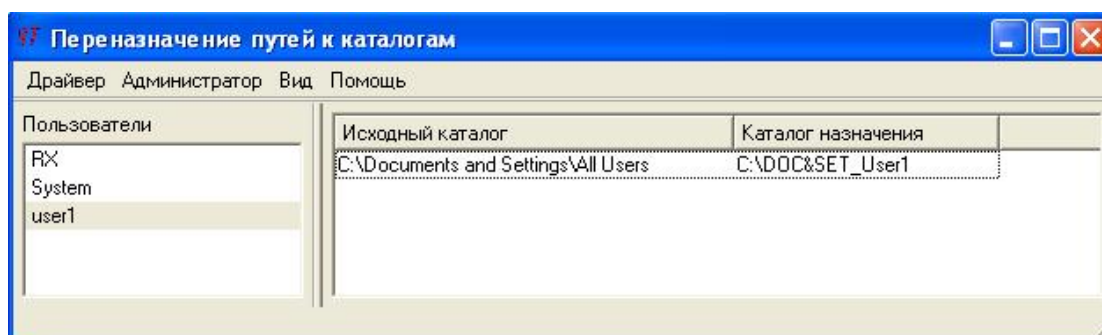
Эти механизмы защиты позволяют средствами КСЗИ реализовать ролевую модель компьютерной безопасности, суть которой состоит в следующем. На одном и том же компьютере один и тот же пользователь может выполнять несколько ролей, например, работа в Интернет с открытой информацией и работа с конфиденциальными данными в локальной сети. Задача – с одной стороны, предотвратить любую возможность утечки конфиденциальных данных, с другой стороны, предотвратить атаки на конфиденциальные данные при работе с открытой информацией, вероятность «заражения» которой вирусами (например, макровирусами, можно рассматривать близкой к 1). Кстати говоря, не сложно буквально «на пальцах» показать, насколько неэффективен для решения этой задачи защиты мандатный принцип контроля доступа, реализуемый большинством средств защиты.

### Решение механизмами защиты КСЗИ:

- Для каждого пользователя создается число учетных записей по числу ролей;
- Для каждой учетной записи определяются файловые объекты (папки), в которых будет храниться информация, обрабатываемая в рамках реализации роли;
- Механизмами разграничения доступа к ресурсам, монтирование которых разрешено к системе (файловые объекты, локальные и разделенные в сети, на жестком диске и на внешних накопителях; сетевые ресурсы, принтеры и т.д.), разграничиваются права доступа между учетными записями, применительно к реализации ролевой модели;

- Изолируется возможность обмена информацией между учетными записями различных ролей (в КСЗИ реализуется механизм разделения между учетными записями файловых объектов, не разделяемых системой и приложениями, механизмом разделения буфера обмена – в ОС Windows буфер обмена принадлежит не учетной записи, а «рабочему столу» - не разделяется системой при многопользовательском режиме, например, при запуске программы по правой кнопке «мыши» под другой учетной записью).

Интерфейс настройки механизма КСЗИ, реализующего разделение между учетными записями файловых объектов, не разделяемых системой и приложениями (любых файловых объектов), приведен на рис.3.



**Рис. 3. Интерфейс механизма переназначения путей к каталогам**

Данный механизм защиты КСЗИ позволяет разделить любую папку между учетными записями. При этом для каждой учетной записи создается собственная папка, в которую для нее перенаправляются обращения, осуществляемые под данной учетной записью к исходной неразделяемой системой, либо приложением, папке. Исходная же папка становится «виртуальной», к ней невозможно обратиться ни под одной учетной записью.

Без данного механизма защиты невозможно корректно реализовать любую разграничительную политику доступа к ресурсам, а уж тем более ролевую модель компьютерной безопасности.



**Замечание.** С целью упрощения задачи администрирования средства защиты, в КСЗИ принципиально изменен (по сравнению с реализацией в современных ОС) подход к построению интерфейсов настройки механизмов защиты – права доступа назначаются пользователям, а не присваиваются объектам, минимизировано число атрибутов доступа (многие из которых устанавливаются системой автоматически), исключена сущность «Владения», как таковая и т.д.

Интерфейс настройки механизма КСЗИ, реализующего разграничения прав доступа пользователей (учетных записей) к файловым объектам, представлен на рис.4.

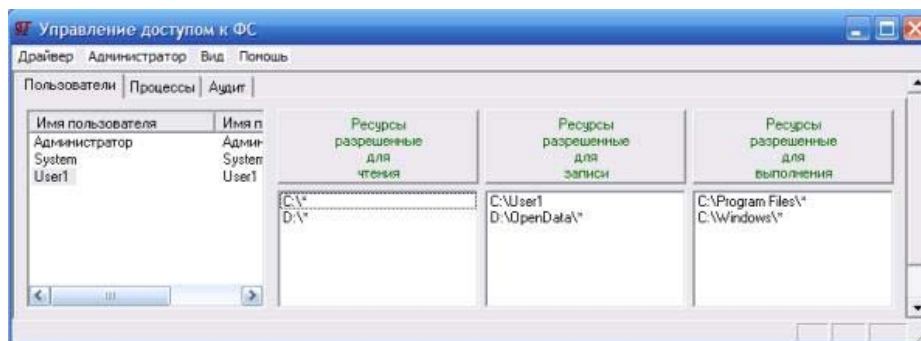


Рис.4. Интерфейс настройки разграничений прав доступа пользователей к объектам файловой системы

Из рис.4 видно, что разграничительная политика формируется назначением прав доступа пользователям (учетным записям). Основу составляет разрешительная разграничительная политика – «Все, что не разрешено – явно не указано, то запрещено» - это единственно корректная реализация разграничительной политики для корпоративных приложений (кстати говоря, реализация которой требуется соответствующим нормативным документом). При этом (см. рис.4) в

одном окне интерфейса отображается вся разграничительная политика доступа ко всем объектам файловой системы (в том числе и к объектам, разделенным в сети, и к объектам на внешних накопителях, включая мобильные), заданная для пользователя (иных прав доступа он не имеет, т.к. они не разрешены по умолчанию, в том числе и для вновь создаваемого объекта). Объект, к которому пользователю разрешается какое-либо право доступа, назначается (с использованием обзора) своим полнопутевым именем. Захотите посмотреть разграничительную политику для другого пользователя, выберите его учетную запись, все разрешенные ему права доступа также будут отображены в одном окне интерфейса. Не требуется перебирать объекты, смотреть на их атрибуты – все наглядно и информативно!

Замечание. Как видно из рис.4, такой сложный механизм защиты, как замкнутость программной среды, задается несколькими записями в интерфейсе (пользователю User1 разрешен запуск программ только из каталогов Windows и Program Files, которые ему запрещено модифицировать – не разрешены для записи).

Для безопасного использования отчуждаемых накопителей (например, Flash-устройств, монтирование которых разрешено к системе), предотвращения раскрытия информации при хищении компьютера или жесткого диска, в КСЗИ используется механизм криптографической защиты файловых объектов (локальных и разделенных в сети, на жестком диске и на внешних накопителях). Реализованные ключевые политики позволяют предотвратить несанкционированное раскрытие похищенной информации, в том числе, и санкционированным пользователем (инсайдером), даже при наличии у последнего ключа шифрования.

Для контроля распечатываемой информации используется механизм теневого копирования информации, отправляемой пользователями на печать.

### **3. Механизмы защиты от атак на уязвимости приложений.**

Основным недостатком механизмов защиты ОС, реализующих разграничительную политику доступа к ресурсам, является возможность разграничений доступа между учетными записями. При этом всеми приложениями (процессами), запускаемыми в системе, наследуются права доступа той учетной записи, от лица которой они запущены.

Реализация данного подхода к защите весьма оправдана в случае реализации ролевой модели компьютерной безопасности, т.е. в предположении, что угроза хищения информации связана непосредственно с пользователем (инсайдером). Вместе с тем, не сложно показать, что приложения несут в себе не менее вероятную самостоятельную угрозу.

Для иллюстрации сказанного, приведем, например, известную укрупненную классификацию вирусных атак:

1. "Вредные программы" (трояны и т.п.). Отдельные программы, которые выполняют те или иные деструктивные/несанкционированные действия.
2. «Вирусы». Программы, обычно не имеющие собственного исполняемого модуля и "живущие" (как правило, заражение осуществляется по средством их присоединения к исполняемому файлу) внутри другого файлового объекта или части физического носителя.
3. «Черви». Разновидность 1,2,4, использующая сетевые возможности для заражения.

4. «Макровирусы» (скриптовые вирусы) - программы, для исполнения которых требуется определенная среда выполнения (командный интерпретатор, виртуальная машина и т.п.). В эту же группу можем отнести и офисные приложения, позволяющие создавать и подключать макросы.

Что же следует из этой классификации? Да то, что угрозу вирусной атаки несет в себе именно процесс, по каким-то причинам реализующий то действие, от которого необходимо защититься.

А теперь введем классификацию процессов, или причин, обуславливающих наше недоверие к определенным группам процессов:

- Несанкционированные (сторонние) процессы. Это процессы, которые не требуются пользователю для выполнения своих служебных обязанностей, и которые могут несанкционированно устанавливаться на компьютер (локально, либо удаленно) с различными целями (эксплойты, реализующие атаки на выявленные в системном и прикладном ПО ошибки, вредоносные, шпионские и т.д. программы). Противодействие возможности их запуска оказывается механизмом обеспечения замкнутости программной среды (см. выше);
- Критичные процессы. К ним мы отнесем две группы процессов: к процессам первой группы отнесем те, которые запускаются в системе с привилегированными правами, например, под учетной записью System, для которой механизмы защиты ОС не реализуют разграничительную политику доступа к ресурсам в полном объеме, к процессам второй группы те, которые наиболее вероятно могут быть подвержены атакам, например, это сетевые службы. Атаки на процессы первой группы наиболее критичны, что связано с возможностью расширения привилегий,

в пределе – получения полного управления системой, атаки на процессы второй группы наиболее вероятны;

- Скомпрометированные процессы – процессы, содержащие ошибки (уязвимости), использование которых позволяет осуществить атаку. Отнесение данных процессов в отдельную группу обусловлено тем, что с момента обнаружения уязвимости и до момента устранения ее разработчиком системы или приложения, может пройти несколько месяцев (известны случаи, что и лет). В течение всего этого времени в системе находится известная уязвимость, поэтому система не защищена;
- Процессы, априори обладающие недеklarированными (документально не описанными) возможностями. К этой группе мы отнесем процессы, являющиеся средой исполнения (прежде всего, это виртуальные машины, являющиеся средой исполнения для скриптов и апплетов, и офисные приложения, являющиеся средой исполнения для макросов).

Таким образом, угрозу атаки, может нести в себе собственно процесс, а причин подобных угроз множество. В подтверждение сказанному немного статистики (за 1 квартал 2008 года, см. рис.5, рис.6).

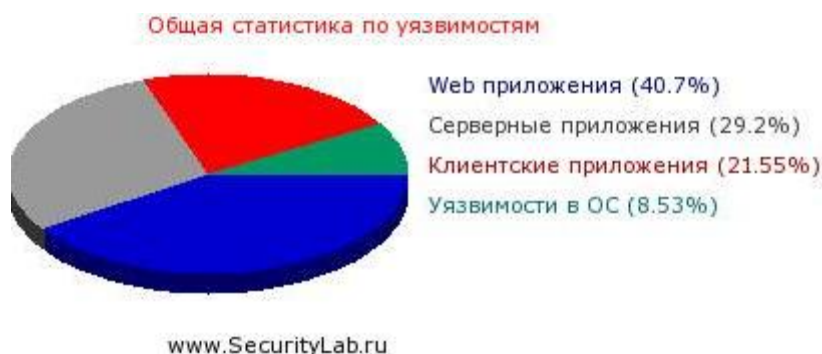


Рис.5



Всего исправлено 505 уязвимостей (57.58%), исправления отсутствуют для 350 уязвимостей (39.91%), для 14 уязвимостей производители опубликовали инструкции по устранению и 8 уязвимостей устранены частично.

**Рис. 6**

Из рис.5 следует, что большинство уязвимостей содержат приложения, а рис.6 иллюстрирует, что подобные уязвимости в приложениях присутствуют всегда.

#### Решение механизмами защиты КСЗИ:

В каждом механизме защиты из состава КСЗИ, реализующем разграничение доступа к ресурсам (к файловым объектам, к объектам реестра ОС, к сетевым ресурсам и т.д.) разграничения могут задаваться, как для учетных записей, так и для процессов, которые в КСЗИ рассматриваются в качестве самостоятельных субъектов доступа, а также для пары «Учетная запись, процесс»).

Данное решение позволяет усекать (по сравнению с правами доступа учетной записи) права доступа процессов (приложений), к которым, по каким-либо причинам, снижено доверие. Используя данную возможность можно защитить от модификации системный диск, объекты реестра ОС, конфиденциальные данные (для критичных процессов может быть создана своя папка, их доступ к папкам, в которых хранятся конфиденциальные данные, им можно запретить, и т.д.

Интерфейс настройки механизма КСЗИ, реализующего разграничения прав доступа процессов к файловым объектам, представлен на рис.7.

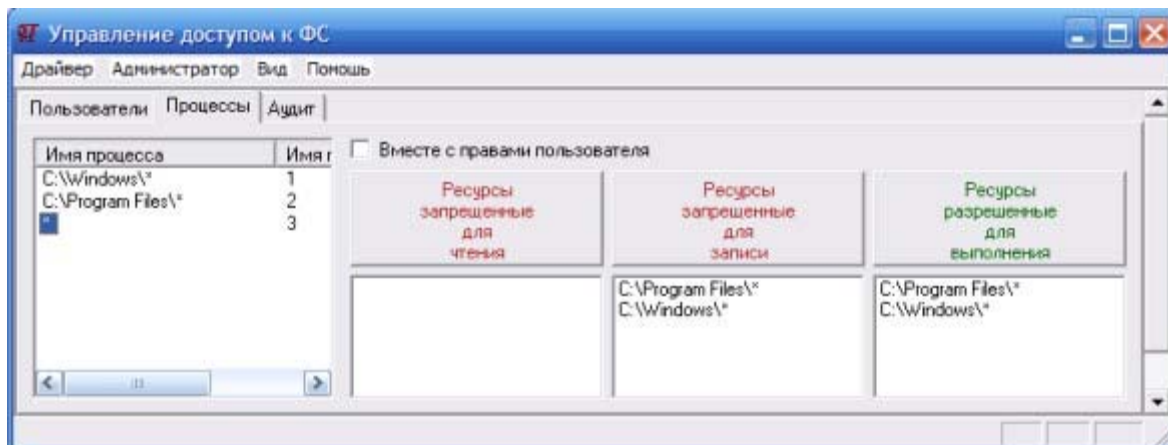


Рис.7. Интерфейс настройки разграничений прав доступа процессов к объектам файловой системы



Замечание. Как видно из рис.7, замкнутость программной среды можно настроить не только для пользователей, но и для процессов (более общее решение).

#### 4. Механизмы защиты от атак на уязвимости ОС.

Следуя современной статистике (за 1 квартал 2008 г., см. рис.8), к наиболее критичным на сегодняшний день могут быть отнесены уязвимости в компонентах ОС, связанные с возможностью повышения привилегий и компрометации системы.

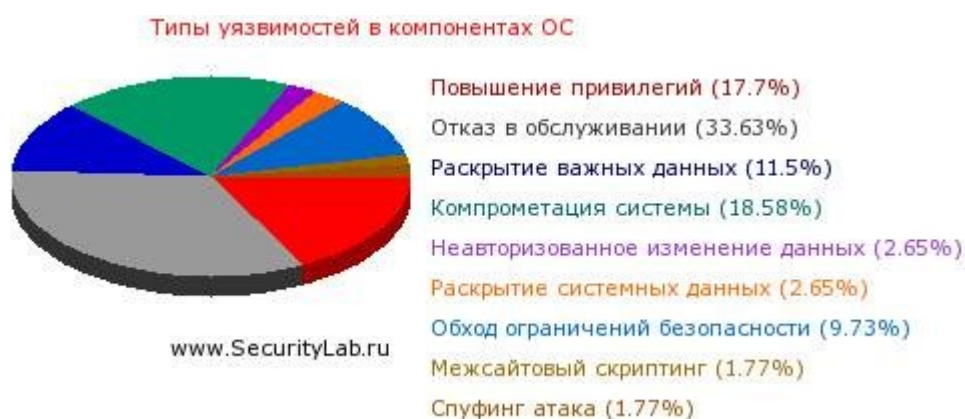


Рис. 8

Возможность компрометации системы обуславливается тем, что средствами ОС невозможно запретить модификацию системного диска в общем случае под любой учетной записью (некоторые приложения должны иметь право записи на системный диск – это право будет запрещено – приложения не смогут функционировать), а для учетной записи System это невозможно в принципе (увидим «синий экран»), т.к. при этом становится запрещен доступ к системному диску «на запись» для всех системных процессов.

Атаки на повышение привилегий связаны с сервисами олицетворения, предоставляемыми ОС разработчикам приложений. Все работающие в системе процессы и потоки выполняются в контексте защиты того пользователя, от имени которого они так или иначе были запущены. Для идентификации контекста защиты процесса или потока используется объект, называемый *маркером доступа* (access

token). В контекст защиты входит информация, описывающая привилегии, учетные записи и группы, сопоставленные с процессом и потоком. При регистрации пользователя, в системе создается начальный маркер, представляющий пользователя, который входит в систему, и сопоставляет его с процессом оболочки, применяемой для регистрации пользователя. Все программы, запускаемые пользователем, наследуют копию этого маркера.

Механизмы защиты, например, в ОС Windows используют маркер, определяя набор действий, разрешенных потоку или процессу. Сервис олицетворения (impersonation) предоставляет возможность отдельному потоку выполняться в контексте защиты, отличном от контекста защиты процесса, его запустившего, т.е. запросить у системы олицетворить себя с правами другого пользователя, в результате - действовать от лица другого пользователя. Эффективное имя пользователя (имя при доступе к ресурсам) может не совпадать с начальным именем пользователя (от лица которого запущен процесс). Как следствие, именно на этом этапе и возникают вопросы корректности идентификации и аутентификации пользователя при запросе доступа к ресурсам, как следствие, корректности реализации разграничительной политики доступа к ресурсам.

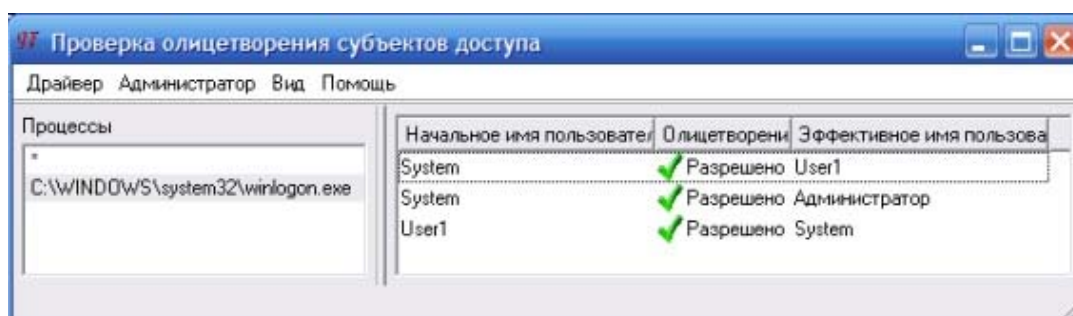
#### **Решение механизмами защиты КСЗИ:**

- Предотвращение возможности компрометации системы достигается реализацией разграничительной политики доступа к файловым объектам и к объектам реестра для процессов (см. выше). КСЗИ предоставляется возможность задавать разграничения для процессов совместные с правами доступа пользователя (по «И»), либо эксклюзивные («по «ИЛИ»). Таким образом, учетной записи System можно запретить право модификации системного диска, а нескольким системным процессам (5-7 для различных ОС), например, winlogon, svchost и др. данное право

доступа разрешить. В результате система будет корректно функционировать, несанкционированно изменить систему и ее настройки становится невозможно даже с системными правами;

- Предотвращение угрозы несанкционированного повышения привилегий реализуется отдельным механизмом защиты КСЗИ – механизмом контроля сервисов олицетворения. Данный механизм позволяет для любого процесса (можно для группы процессов, по маске и т.д.) установить свои собственные разрешенные права олицетворения – смены учетной записи при доступе к ресурсам.

Интерфейс настройки механизма КСЗИ, реализующего контроль сервисов олицетворения, представлен на рис.9.



**Рис. 9. Интерфейс настройки механизма проверки олицетворения субъектов доступа**

Механизм защиты, реализованный в КСЗИ, предполагает возможность назначить разрешительную, либо запретительную политику смены первичного маркера для процессов при обращении к ресурсам (файловые объекты и объекты реестра ОС), т.е. в качестве субъекта доступа здесь выступает процесс (может задаваться полнопутевым именем, именем папки, тогда одинаковые разграничения действуют для всех процессов, запускаемых из этой папки, маской), что обеспечивает максимальную гибкость применения механизма, в качестве объектов разграничений – пара: исходный маркер безопасности (исходное имя пользователя) и маркер безопасности, на который разрешается, либо запрещается

менять исходный маркер (эффективное имя пользователя), под которым и осуществляется доступ к ресурсам.

Настройки механизма, представленные на рис.9, иллюстрируют возможность реализации дополнительных свойств защиты, особенно, если в качестве субъекта доступа рассматривать системные процессы. Для рассмотрения данного примера настройки, напомним, что системным процессом winlogon осуществляется регистрация входа нового пользователя в систему. При регистрации нового пользователя, потоки, запускаемые процессом winlogon (с правами System), олицетворяют себя с правами регистрируемого пользователя. Как следствие, если разрешить для процесса winlogon олицетворение System с определенными учетными записями (см. рис.9), то вход в систему станет возможен только под этими учетными записями, вне зависимости от того, какие еще (санкционировано, либо нет) учетные записи заведены в системе.



**Замечание.** Определение необходимых настроек КСЗИ существенно упрощается с использованием механизма инструментального аудита, позволяющего достаточно просто определиться с ресурсами, к которым необходимо разрешить доступ любого процесса (приложения) для обеспечения корректности его функционирования.

***Данный краткий обзор реализованных в КСЗИ «Панцирь-К» технологий защиты отнюдь не преследует цели описать все возможности средства защиты. Рассмотрены лишь отдельные механизмы защиты, позволяющие оценить функциональные возможности КСЗИ, эффективность ее применения в современных условиях.***

### **Как сравнить КСЗИ «Панцирь-К» с иными средствами защиты?**

На самом деле, очень просто. Попробуйте найти в ином средстве, по крайней мере, те механизмы защиты (либо подобные им) из состава КСЗИ «Панцирь-К», которые описаны выше. Если не найдете, то задайте себе вопрос: для чего предназначено рассматриваемое Вами иное средство, если им не решаются ключевые задачи защиты информации?