Программно-технические средства защиты от несанкционированного доступа для платформы Microsoft Windows Vista / Windows Server 2008 «Protect»

Software and hardware protection tools from unauthorised access for Microsoft Windows Vista / Windows Server 2008 «Protect» platform

Ключевые слова: несанкционированный доступ – unauthorised access; модель контроля доступа – access check model; дискреционная и мандатная модели – discretionary and mandatory model; поле метаданных – metadata field.

Статья посвящена современному программно-аппаратному комплексу средств многофакторной аутентификации для операционных систем на базе электронных ключей для шины USB, рассчитанных на применение как в государственных, так и в коммерческих организациях.

The article is dedicated to modern software and hardware complex of multi-factor authentication for operating systems based on electronic keys for the USB bus is designed for use in both the public and commercial organizations.

ПРИСЯЖНЮК / PRISYAZHNIUK А.
Андрей Сергеевич
(office@itain.spb.ru)
кандидат технических наук,
заместитель генерального директора
ЗАО «Институт телекоммуникаций»,
Санкт-Петербург

КАРМАНОВ / KARMANOV А.
Андрей Геннадьевич
(office@itain.spb.ru)
кандидат технических наук, доцент,
ЗАО «Институт телекоммуникаций»,
Санкт-Петербург

ВВЕДЕНИЕ

В связи с растущим объемом электронного документооборота в государственных организациях повышается актуальность задачи защиты секретной информации от несанкционированного доступа третьих лиц. Решение данной задачи на рабочих местах, использующих операционную систему Windows Vista, требует применения дополнительных технических средств защиты. Основным критерием разрабатываемого решения является соответствие требованиям РД ФСТЭК РФ для систем, в которых хранятся или обрабатываются сведения, составляющие государственную тайну, а также конфиденциальная информация при обеспечении удобства эксплуатации и развертывания.

Комплекс программных средств «Protect» ориентирован на задачи государственных предприятий, которые используют в своей работе сведения, составляющие государственную тайну и конфиденциальную информацию. Предназначение продукта – создание на базе рабочих станций, работающих под управлением операционных систем Microsoft Windows, защищенной информационной среды, которая будет соответствовать требованиям по безопасности, предъявляемым к средствам защиты от несанкционированного доступа при работе с особыми видами документов. В зависимости от модификации, продукт планируется использовать для защиты сведений, представляющих конфиденциальную информацию и государственную тайну, включая секретные документы. Планируется проведение сертификации различных модификаций продукта на соответствие требованиям ФСТЭК РФ, предъявляемым к средствам защиты от несанкционированного доступа для защиты указанных категорий документов.

В связи с введением закона «О персональных данных» каждый обработчик должен защищать персональные данные, которые обрабатывает. Таким образом, нами предлагается программное обеспечение, в рамках которого разрабатываются

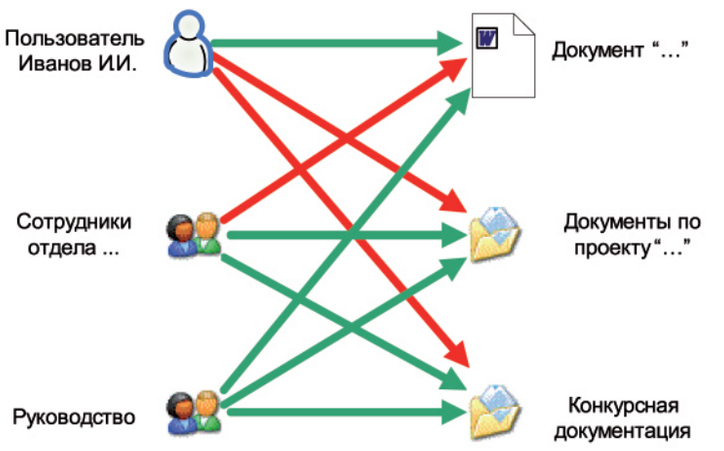

Рис. 1. Пример использования дискреционной модели контроля доступа
(зелеными стрелками отмечены разрешенные виды обращений пользователей к документу,
красными – запрещенные)

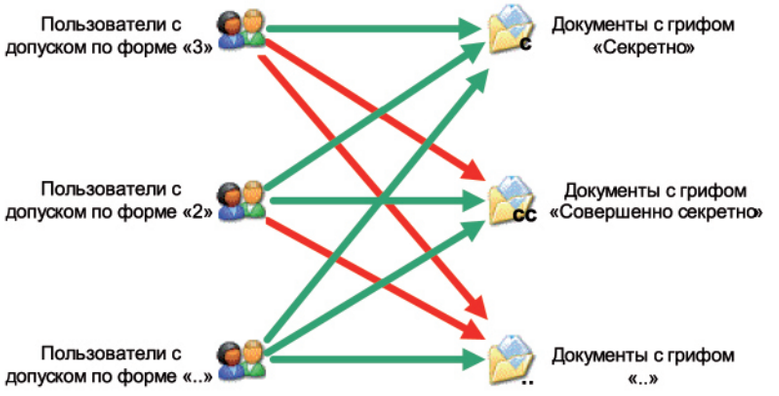

Рис. 2. Пример мандатной модели контроля доступа
(зелеными стрелками отмечены разрешенные виды обращений пользователей к документу,
красными – запрещенные)

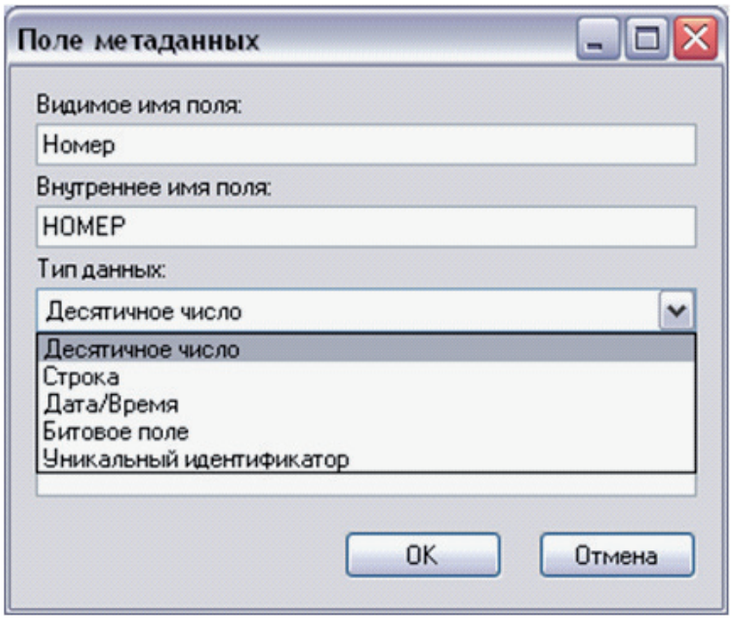

Рис. 3. Создание поля метаданных

математические модели, методы и алгоритмы автоматизации процессов анализа и выбора элементов системы защиты информации (СЗИ), создание научно-методических основ защиты информации при ее обработке с учетом особенностей объекта. Проще говоря, потребитель устанавливает у себя клиент, составляет технический план с нанесением объектов информационной обработки, моделирует объект и получает рекомендации по построению оптимальной СЗИ: максимальный эффект при определенных затратах, проверяет объект на соответствие нормативно-правовым актам по защите персональных данных. Все это позволит ответить на вопросы: «Как защищать?», «Где защищать?», «Когда защищать?», «Каким образом защищать?», т.е. создать концепцию информационной безопасности на объекте как основного руководящего документа с учетом всех нормативно-правовых актов. А также избежать ошибок, просчетов при проектировании СЗИ и защититься от претензий надзорных органов.

РАЗГРАНИЧЕНИЕ ДОСТУПА И МАРКИРОВКА ДОКУМЕНТОВ

При разграничении доступа к документам применяются две основные модели разграничения доступа: дискреционная и мандатная. Каждая из них имеет свои преимущества: так, например, мандатная позволяет разрешить работу с документом только тем категориями сотрудников, которые имеют соответствующую форму допуска. Это снимает необходимость настраивать разрешения доступа к документу для каждого конкретного сотрудника. Вместе с тем необходимость работы с конкретным документом обычно есть не у всех сотрудников, которые имеют соответствующую форму допуска. В таких случаях дискреционная модель позволит дополнительно ограничить число допущенных конкретными сотрудниками или подразделениями.

ДИСКРЕЦИОННАЯ МОДЕЛЬ КОНТРОЛЯ ДОСТУПА

Дискреционная модель разграничения прав доступа предусматривает распределение полномочий на основе индивидуальных прав доступа каждого пользователя или учетной группы пользователей к тому или иному документу. Рассмотрим пример дискреционной модели разграничения прав доступа, ппоказанный на рис. 1.

МАНДАТНАЯ (ПОЛНОМОЧНАЯ) МОДЕЛЬ КОНТРОЛЯ ДОСТУПА

Мандатная модель подразумевает присваивание субъектам безопасности тех или иных категорий полномочий. Рассмотрим классический пример такой модели (рис. 2) – грифы секретности документов, где пользователи должны иметь категорию допуска, соответствующую категории секретности документа. В мандатной модели категории полномочий могут быть как независимыми одна от другой, так и образовывать иерархию. Таким

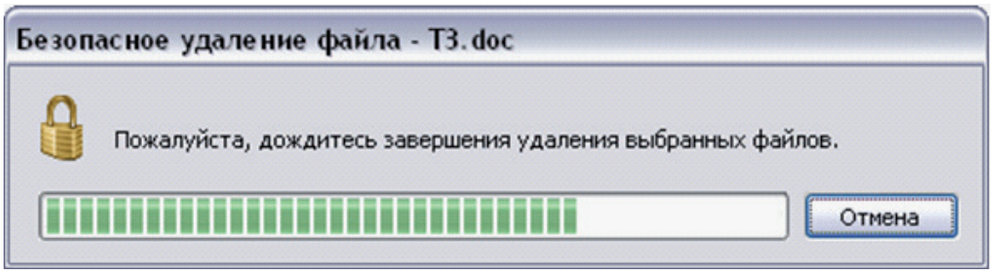

Рис. 4. Окно безопасного удаления файла

образом, в рассмотренном примере пользователи, имеющие допуск по форме «2», могут работать не только с документами, имеющими гриф «СС», но и с документами с грифом «С».

Несмотря на то, что поддержка мандатной модели контроля доступа требуется РД ФСТЭК только при работе с секретными документами, она является также функционально востребованной при обработке конфиденциальной информации.

МАРКИРОВКА ДОКУМЕНТОВ

Функция маркировки документов позволяет хранить вместе с документом дополнительную информацию, такую как его номер, дату утверждения или срок действия грифа. Информация впоследствии может быть просмотрена пользователями при работе с документом.

Набор полей метаданных, которые будут использоваться, задается при установке продукта, что позволяет дополнять его теми видами информации, которые необходимы для конкретной организации. Для этого на этапе установки в специальном окне (рис. 3) необходимо указать видимое имя поля (то, которое будет показано пользователям), тип хранимых данных и внутреннее имя поля, которое будет использовано для идентификации при переносе документа между компьютерами.

БЕЗОПАСНОЕ УДАЛЕНИЕ ИНФОРМАЦИИ

Во многих случаях после удаления файлов с жесткого диска (включая удаление из «Корзины») сохраняется возможность их последующего восстановления. Существует вероятность использования этой особенности злоумышленником для получения несанкционированного доступа к информации. Вследствие этого в составе программного комплекса «Protect» предусмотрена возможность невосстановимого удаления файлов и очистки свободного пространства жесткого диска от остаточной информации.

В зависимости от учетной категории документа и установленных администратором политик, при удалении документа стандартными средствами Windows вместо обычной процедуры удаления будет автоматически применена процедура безопасного удаления. Окно удаления документа показано на рис. 4.

ОГРАНИЧЕНИЕ ДОСТУПА К ОТЧУЖДАЕМЫМ НОСИТЕЛЯМ И ВНЕШНИМ УСТРОЙСТВАМ

Во многих случаях возникает необходимость полностью запретить доступ пользователей к той или иной категории устройств компьютерной периферии либо ограничить его в соответствии с дискреционной или мандатной моделью. В рамках комплекса разработана подсистема контроля доступа к устройствам и съемным накопителям информации, в числе которых можно выделить следующие категории устройств:

– оптические дисководы (CD-R/RW или DVD-R/RW);

– USB-flash накопители и прочие устройства хранения данных, подключаемые через USB (внешние жесткие диски, устройства чтения карт памяти и т.п.);

– floppy-дисководы;

– съемные магнитные диски высокой емкости (ZIP);

– извлекаемые жесткие диски;

– принтеры.

Программный продукт предоставляет возможность ограничения доступа к отчуждаемым носителям. В случае если доступ к какой-либо из перечисленных категорий устройств был ограничен, устройства перестают определяться компьютером.

ИНТЕГРАЦИЯ В ОПЕРАЦИОННУЮ СИСТЕМУ WINDOWS

Одним из существенных критериев для удобства использования пакета средств защиты от несанкционированного доступа является степень его интеграции в стандартные средства опера-

ционной системы. Для решения этой задачи в составе комплекса были разработаны специализированные расширения оболочки Windows для управления учетными категориями документов, а также визуального отображения принадлежности документа к той или иной учетной категории. Кроме того, продукт позволяет при удалении документов определенных учетных категорий автоматически задействовать функцию безопасного удаления вместо стандартных процедур удаления операционной системы Microsoft Windows. Также необходимо отметить, что установка программного продукта не препятствует нормальному функционированию операционной системы.

ПРОВЕРКА ЦЕЛОСТНОСТИ КОНФИГУРАЦИИ СВТ

Программный продукт обеспечивает контроль подлинности основных аппаратных компонентов рабочей станции на предмет несанкционированной подмены путем проверки их серийных номеров. Кроме того, контролируется целостность конфигурации программных средств защиты на предмет несанкционированного изменения. Для проверки целостности конфигурации СВТ разработана специальная системная служба Windows, осуществляющая проверку моделей и серийных номеров устройств во время запуска операционной системы.

УСТАНОВКА И РАЗВЕРТЫВАНИЕ

Установка программного продукта выполняется специализированной установочной программой. Процесс установки аналогичных продуктов, как правило, является достаточно трудоемким вследствие необходимости указания большого числа настроек, что не позволяет проводить одновременную автоматическую установку подобных продуктов на большом числе рабочих мест. Для устранения данной проблемы было разработано решение, позволяющее однократно ввести необходимые настройки через графический интерфейс и сформировать файл шаблона установки, который впоследствии может быть использован для автоматической установки программного продукта через локальную сеть, либо при ее отсутствии загрузить все установки из файла вручную.

ВЫВОДЫ

Программный комплекс «Protect» успешно решает основные задачи в области защиты от несанкционированного доступа к информации на рабочих местах, использующих операционные системы Microsoft Windows Vista/Server 2008, обеспечивает удобство установки. Кроме того, обеспечена интеграция средств защиты в оболочку и средства защиты операционной системы Windows, что упрощает использование и настройку.

Литература

1. *Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю.* Теоретические основы компьютерной безопасности. – М.: «Радио и связь», 2000.
2. *Петраков А.В.* Основы практической защиты информации. – М.: «Радио и связь», 2003.
3. *Белкин П.Ю., Михальский О.О.* Защита программ и данных. – М.: «Радио и связь», 2004.
4. *Шаньгин В.Ф., Дшхунян В.Л.* Электронная идентификация. – М., 2004.
5. *Кузовкин К.Н.* Защищенная платформа для Web-приложений. – М., 2005.
6. *Олифер Н.А., Олифер В.Г.* Стратегическое планирование сетей масштаба предприятия. – М., 1997.
7. *Смит Э.Р.* Аутентификация: от паролей до открытых ключей. – М.: ИД «Вильямс», 2002.
8. Microsoft Corporation. Microsoft Windows 2000 Professional. – М.: ИД «Русская редакция», 2003.