УДК 004.056.53
DOI 10.21685/2587-7704-2017-2-2-3

Open Access REVIEW

Анализ функциональных возможностей программных средств защиты информации

В. А. Губарева
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. А. Авдеев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Рассмотрены различные средства защиты информации от несанкционированного доступа. Описаны их предназначение и возможности. Приведена классификация защищенности автоматизированных систем.

Ключевые слова: информационная безопасность, автоматизированная система, средство защиты, несанкционированный доступ, конфиденциальная информация, персональные данные.

Analysis of functional possibilities of IPS software

V. A. Gubareva
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. A. Avdeev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. Various means of information protection from unauthorized access are considered, and their purpose and capabilities are described. The protection classification of automated systems is suggested.

Key words: information security, automated system, means of protection, unauthorized access, confidential information, personal data.

В настоящее время в современном обществе возрастает роль информационной сферы. Наравне с этим возрастает необходимость защиты данных, что делает актуальной проблему обеспечения информационной безопасности. Одной из основных задач, решение которых необходимо в интересах обеспечения информационной безопасности, является развитие системы защиты информации, совершенствование ее организации, также потеря данных может привести как к раскрытию конфиденциальных сведений, так и к раскрытию коммерческой информации, что может привести к реализации угроз экономической безопасности [1].

Задача защиты информации от несанкционированного доступа (НСД) может быть решена использованием средств защиты информации (СЗИ), таких как «Страж NT», «Secret Net», «Аккорд». Охарактеризуем данные программные продукты.

СЗИ от НСД «Secret Net» разработан компанией «Код безопасности». Основные функции, реализуемые системой «Secret Net»:

– контроль входа пользователей в систему;

– разграничение доступа пользователей к устройствам компьютера;

– создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера;

– разграничение доступа пользователей к конфиденциальной информации;

– контроль вывода на печать и добавление грифов в распечатываемые документы (маркировка документов);

– контроль целостности защищаемых ресурсов;

– контроль подключения и изменения устройств компьютера;

– уничтожение (затирание) содержимого файлов при их удалении;

– теневое копирование выводимой информации;

– регистрация событий безопасности в журнале «Secret Net»;

– мониторинг и оперативное управление защищаемыми компьютерами;

– централизованный сбор и хранение журналов;

– централизованное управление параметрами механизмов защиты.

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа, разработанный компанией ОКБ САПР, «Аккорд» предназначен для применения на средствах вычислительной техники (СВТ), функционирующих под управлением ОС Windows NT, Windows 2000, Windows 2000 Server, Windows XP, Windows 2003 Server, Windows Vista, Windows 2008 Server, Windows 7 с целью обеспечения защиты от несанкционированного доступа к СВТ и автоматизированной системе (АС) на их основе при многопользовательском режиме эксплуатации. Комплекс СЗИ от НСД «Аккорд» обеспечивает:

– защиту от несанкционированного доступа к АС (СВТ) и ее ресурсам;

– разграничение доступа к ресурсам СВТ, управлением потоками информации в соответствии с уровнем полномочий пользователей, используя дискреционный и мандатный способы управления доступом пользователей;

– защиту от несанкционированных модификаций программ и данных и различного рода проникающих разрушающих воздействий (ПРВ);

– контроль целостности конфигурации технических средств СВТ, программ и данных с реализацией пошагового алгоритма контроля целостности;

– создание изолированной программной среды (ИПС) с исключением возможности несанкционированного выхода в ОС, загрузки с FDD и несанкционированного прерывания контрольных процедур с клавиатуры;

– ввод широкого перечня дополнительных защитных механизмов в соответствии с политикой информационной безопасности, принятой в организации.

Система защиты информации от несанкционированного доступа, разработанная ООО «РУБИНТЕХ», «Страж NT» (версия 3.0), представляет собой комплекс средств защиты информации в автоматизированных системах на базе персональных компьютеров.

С помощью СЗИ «Страж NT» обеспечивается реализация требований по защите информации от несанкционированного доступа в системах обработки персональных данных, применяется при аттестации объектов информатизации. СЗИ «Страж NT» функционирует в среде операционных систем Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 и устанавливается как на автономных рабочих местах, так и на рабочих станциях и файл-серверах локальной вычислительной сети, а также на кластерных системах.

В СЗИ «Страж NT» реализована смешанная разрешительно-запретительная модель защиты информации, означающая, что для отдельных механизмов защиты применяется разрешительная политика, а для других – запретительная. Система защиты состоит из следующих основных подсистем:

– идентификации и аутентификации;

– разграничения доступа;

– контроля потоков информации;

– управления запуском программ;

– управления защитой;

– регистрации событий;

– маркировки документов;

– контроля целостности;

– учета носителей информации;

– преобразования информации на отчуждаемых носителях;

– контроля устройств;

– тестирования системы защиты.

Для установки, настройки и управления функционированием СЗИ «Страж NT» должен быть назначен администратор системы защиты. Пользователь, выполняющий функции администратора системы защиты, должен быть создан перед началом установки системы защиты стандартными средствами операционной системы [2].

Достоинствами СЗИ от НСД «Страж NT» являются:

– низкая стоимость относительно стоимости аналогичных СЗИ от НСД («Secret Net», «Аккорд»);

– возможность устанавливать как на отдельные персональные электронно-вычислительные машины (ПЭВМ), так и по локальной вычислительной сети (ЛВС);

– гибкая настройка – существует возможность использования шаблонов для упрощения настройки. Шаблоны могут быть как от разработчиков, так и свои собственные, созданные на основе шаблонов от разработчиков. Пример шаблона приведен на рис. 1;

– журнал регистрации событий отображает полную информацию о событиях, есть возможность использования фильтров для поиска определенных событий;

– простота в эксплуатации настроенной СЗИ от НСД.

Путь к ресурсу	Фильтр	Гриф и режим запуска	Применить
%APPDATA%\Microsoft\Access		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%APPDATA%\Microsoft\Excel		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%APPDATA%\Microsoft\Office		Без проверки\Запрещён	Для этой папки и её файлов
%APPDATA%\Microsoft\Office\Последние файлы		Без проверки\Запрещён	Только для этой папки
%APPDATA%\Microsoft\OIS		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%APPDATA%\Microsoft\Proof		Без проверки\Запрещён	Для этой папки и её файлов
%APPDATA%\Microsoft\Publisher		Без проверки\Запрещён	Для этой папки и её файлов
%APPDATA%\Microsoft\Word		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%APPDATA%\Microsoft\InfoPath		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%APPDATA%\OneNote		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%APPDATA%\Microsoft\Publisher Building Blocks		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%APPDATA%\Microsoft\Publisher		Без проверки\Запрещён	Для этой папки и её файлов
%APPDATA%\Microsoft\UProof		Без проверки\Запрещён	Для этой папки и её файлов
%APPDATA%\Microsoft\Word		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%APPDATA%\Microsoft\Шаблоны		Без проверки\Запрещён	Для этой папки и её файлов
%USERPROFILE%\Local Settings\Application Data		Без проверки\Запрещён	Для этой папки и её файлов
%USERPROFILE%\Local Settings\Application Data\Microsoft\Office		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%USERPROFILE%\Local Settings\Application Data\Microsoft\OIS		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%USERPROFILE%\Local Settings\Temp\OIS		Без проверки\Запрещён	Для этой папки, её подпапок и файлов
%USERPROFILE%\Local Settings\Temporary Internet Files\Content.MSO		Без проверки\Запрещён	Для этой папки и её файлов
%USERPROFILE%\Local Settings\Temporary Internet Files\Content.Word		Без проверки\Запрещён	Для этой папки и её файлов
%ProgramFiles%\Microsoft Office\Office14\STARTUP		Без проверки\Запрещён	Для этой папки, её подпапок и файлов

Рис. 1. Пример шаблона

Недостатки СЗИ от НСД «Страж NT»:

– трудности в настройке специфического программного обеспечения;

– при нарушении контроля целостности предыдущее значение не восстанавливается;

– сложности при записи учтенных носителей CD и DVD.

С помощью СЗИ «Страж NT» обеспечивается реализация требований по защите информации от несанкционированного доступа в системах обработки персональных данных, применяется при аттестации объектов информатизации, также СЗИ имеет сертификат ФСТЭК России, который позволяет использовать ее при создании автоматизированных систем до класса защищенности 1Б включительно и для защиты информации в информационной системе персональных данных (ИСПДн) до 1-го класса включительно.

Выбор класса автоматизированной системы производится заказчиком и разработчиком с привлечением специалистов по защите информации. Устанавливается девять классов защищенности АС от несанкционированного доступа к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы делятся на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС. Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А. Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А. Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и

(или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов: 1Д, 1Г, 1В, 1Б и 1А [3].

После установки СЗИ «Страж NT» используются различные программы, предназначенные для проверки и тестирования программного обеспечения АРМ. Одной из таких программ является программа ФИКС. Эта программа фиксации и контроля исходного состояния программного комплекса, предназначена для выполнения следующих функций:

– фиксации исходного состояния файлов программного комплекса;
– контроля исходного состояния программного комплекса;
– фиксации и контроля каталогов;
– контроля различий в заданных файлах;
– контроля целостности файлов программного комплекса.

В процессе работы «ФИКС 2.0.1» осуществляет контроль целостности собственных файлов. В случае обнаружения попыток несанкционированного их изменения программа перестает работать.

Программа «ФИКС 2.0.1» может работать в следующих режимах:

– фиксации исходного состояния;
– контроля целостности;
– фиксации и контроля каталогов;
– контроля исходного состояния комплексов;
– сравнения файлов.

Пример настройки программы «ФИКС 2.0.1» приведен на рис. 2.

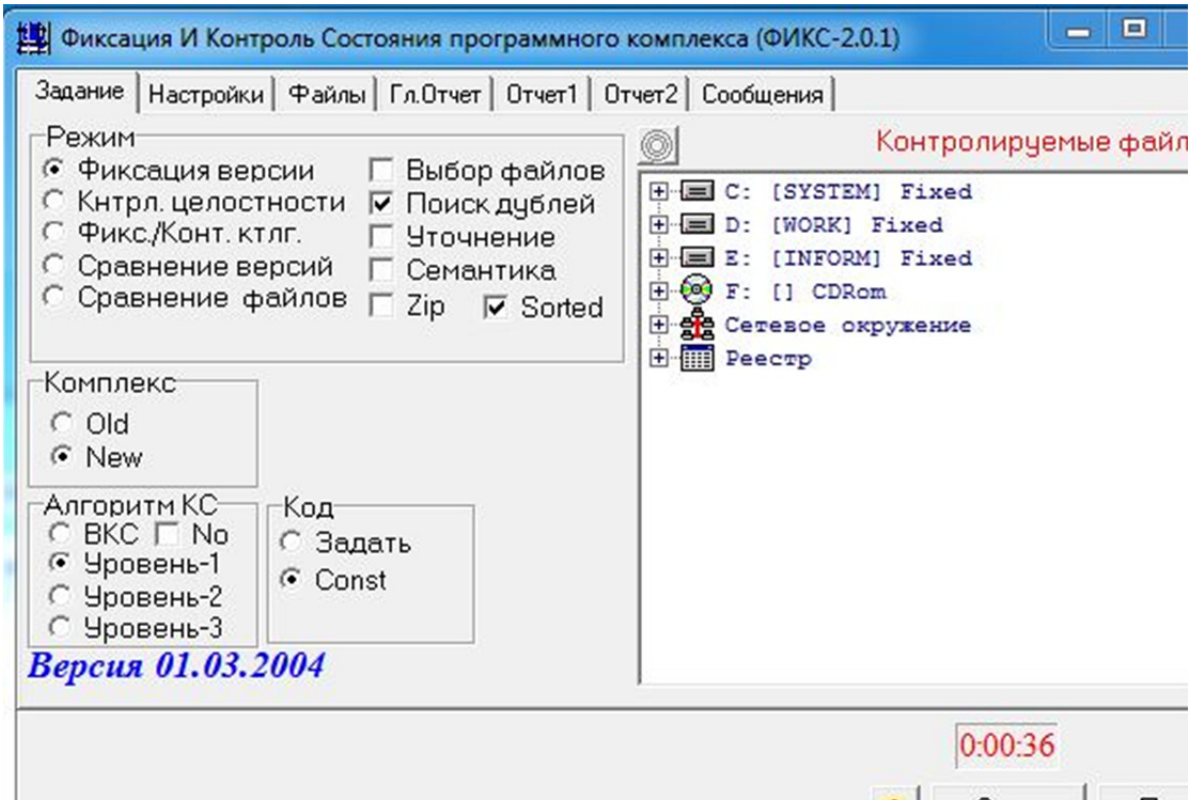

Рис. 2. Программа «ФИКС 2.0.1»

Проанализировав системы, можно сделать вывод, что все они могут применяться для защиты информации. Однако важной особенностью СЗИ «Страж NT» является возможность использования шаблонов уже готовых и созданных вручную для упрощения настройки.

Заключение

С помощью СЗИ «Страж NT» обеспечивается реализация требований по защите информации от несанкционированного доступа в системах обработки персональных данных [4], применяется при аттестации объектов информатизации, также СЗИ имеет сертификат ФСТЭК России, позволяющий использовать ее при создании автоматизированных систем до класса защищенности 1Б включительно и для защиты информации в ИСПДн до 1-го класса включительно. Применение СЗИ «Страж NT» в

комплексе с «ФИКС 2.0.1» позволяет не только обеспечивать безопасность (конфиденциальность) данных, но контролировать целостность информации.

Библиографический список

1. Сергеева, И. А. Промышленная политика и экономическая безопасность России / И. А. Сергеева // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2015. – № 1 (33). – С. 258–267.
2. Система защиты информации от несанкционированного доступа «Страж NT» Версия 3.0. Описание применения. – URL: http://www.guardnt.ru/download/doc/app_guide_nt_3_0.pdf
3. Программа фиксации и контроля исходного состояния программного комплекса (ФИКС 2.0.1). Описание применения.
4. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – URL: http://fstec.ru/component/attachments/download/296

Губарева, В. А.
Анализ функциональных возможностей программных СЗИ / В. А. Губарева, А. А. Авдеев // Инжиниринг и технологии. – 2017. – Vol. 2(2). – DOI 10.21685/2587-7704-2017-2-2-3