УДК 004.4

Кувшинов Н.Е., инженер научно-исслед. лаборатории «ФХПЭ»

Казанский государственный энергетический университет

Россия, г. Казань

Kuvshinov N.E., engineer laboratory "FHPE"

Kazan State Power Engineering University

Russia, Kazan

ЗАЩИТНЫЕ СРЕДСТВА В ОС

Аннотация: Статья посвящена рассмотрению защитных средств в операционных системах, а также дефектам обеспечения безопасности данных в системе. Для этого в статье проведен сравнительный анализ защищенности ОС семейства Windows.

Ключевые слова: операционная система, функциональные дефекты ОС, встроенная защита, защитные средства операционных систем.

PROTECTIVE MEANS IN OPERATING SYSTEMS

Annotation: The article is devoted to the consideration of protective means in operating systems, as well as to the defects in ensuring the security of data in the system. To do this, the article compares the security of the Windows operating system.

Keywords: operating system, functional OS defects, built-in protection, operating system protection.

Операционная система – специально санкционированная совокупность программ, которая управляет ресурсами системы для более действенного их применения, а также гарантирует интерфейс пользователя с ресурсами [1].

Переход к мультипроцессорной организации средств ВТ начал осуществляться к концу 60-х гг. XX в. К этому периоду трудности распределение ресурсов и их защиты стали более острыми и трудноразрешимыми. Решение этих проблем привело к соответственной

организации ОС и широкому использованию аппаратных средств защиты (защита памяти, аппаратный контроль, диагностика и т.п.).

На сегодняшний день существует достаточно большая статистика угроз ОС, которая ориентирована на преодоление встроенных в ОС механизмов защиты, позволяющих изменить настройки механизмов безопасности, обойти разграничения доступа и т.д.

Таким образом, большинство распространенных систем довольно проблематичны с точки зрения безопасности. И это несмотря на отчетливую тенденцию к повышению уровня защищенности этих систем.

Механизм защиты ОС – все средства и механизмы защиты данных, функционирующие в составе ОС. Операционные системы, в составе которых функционируют средства и механизмы защиты данных, часто называют защищенными системами.

Под безопасностью ОС следует понимать такое состояние ОС, при котором невозможно случайное или преднамеренное нарушение функционирования ОС, а также нарушение безопасности находящихся под управлением ОС ресурсов системы [2].

Основной проблемой обеспечения безопасности ОС является проблема создания механизмов контроля доступа к ресурсам системы. Процедура контроля доступа заключается в проверке соответствия запроса субъекта предоставленным ему правам доступа к ресурсам.

Основная масса ОС обладает дефектами, именно с точки зрения обеспечения безопасности данных в системе, что вызвана выполнением задачи обеспечения максимальной доступности системы для пользователя.

Рассмотрим стандартные функциональные дефекты ОС, которые могут привести к созданию каналов утечки данных [3].

1. Идентификация. Каждому ресурсу в системе должно быть присвоено уникальное имя, то есть индивидуальный номер. Во множества

системах пользователи не имеют способности удостовериться в том, что используемые ими ресурсы действительно принадлежат системе.

2. Пароли. Практически все пользователи выбирают простейшие пароли, которые легко подобрать или угадать.

3. Перечень паролей. Хранение списка паролей в незашифрованном виде дает возможность его компрометации с последующим НСД к данным.

4. Пороговые значения. Для того чтобы предотвратить попытки несанкционированного входа в систему с помощью подбора пароля следует ограничить количество таких попыток, что в некоторых ОС не учтено.

5. Подразумеваемое доверие. Во многих случаях программы ОС считают, что иные программы работают верно.

6. Общая память. При применении общей памяти не всегда после выполнения программ очищаются участки оперативной памяти (ОП).

7. Разрыв связи. В подобном случае ОС обязана незамедлительно завершить сеанс работы с пользователем или повторно установить достоверность субъекта.

8. Передача данных по ссылке, а не по значению. В аналогичных случаях возможно хранение характеристик в ОП после контроля их точности, нарушитель содержит право реконструировать эти данные до их применения.

9. Система имеет возможность содержать большое количество элементов (например, программ), имеющих различные преимущества.

На сегодняшний день, наиболее известными операционными системами являются Windows, Mac OS и семейство операционных систем Linux.

Теперь более подробно остановимся на основных механизмах защиты, реализованных в ОС семейства Windows 7 и Windows 8[4, 5], и проведем сравнительный анализ защищенности ОС семейства Windows.

Таблица 1 Сводная информация о встроенной защите Windows 7 и Windows 8

	Компонент	Windows 7	Windows 8
Загрузка системы	UEFI	-	+
	ASLR	+	+*
	ELAM	-	+
	Управление автозагрузкой	+	+*
	Вход систему с помощью альтернативных паролей	-	+
Во время работы	Защитник	+	+*
	Брандмауэр	+	+
	SmartScteen	+	+*
	Запуск приложений в песочнице	-	+
	UAC	+	+
	Подсчет сетевого трафика	-	+
Дополнительно	Родительский контроль	+	+*
	Резервное копирование	+	+
	Шифрование	+	+
	Установка на накопитель	-	+
	Виртуализация	-	+

* – функция реализована лучше.

Внутренняя защита Windows 7 и Windows 8 основывается по модульному принципу, т.е. это не один продукт, а комплект

взаимодействующих компонентов. В таблице ряд модулей помечен звездочкой, это свидетельствует о том, что «функция реализована лучше» в Windows 8. Несмотря на то, что данная функция присутствует в обеих версией операционной системы, реализация в Windows 8 оказалась полнее и оптимальнее. Для того чтобы понять какая из операционных систем является более защищенной перейдем более к подробному анализу.

Загрузка системы UEFI – стандартизированный распространяемый интерфейс вставки. По сущности, это независимая легкая операционная система, которая представляет собой интерфейс между ведущей ОС и микропрограммами, важнейшей задачей которого считается корректная инициализация оборудования и передача управления загрузчику ведущей ОС, установленной на компьютере.

Одними из главных и востребованных особенностей UEFI – «безопасная загрузка», низкоуровневая криптография, сетевая аутентификация, универсальные графические драйверы и еще многое другое. В свою очередь, функция SecureBoot в Windows 8 разрешает в процессе загрузки реализовать проверку всех запускаемых компонентов (драйвера, программы), гарантируя, что лишь доверенные программы смогут производиться в процессе загрузки ОС.

ASLR – технология рандомизации адресного пространства. Она отвечает за защиту системы от эксплуатации багов в памяти. Разработка случайным образом сдвигает данные и программный код в памяти для более сложной реализации эксплоитов. Создатели реализовали её и в Windows 8, и в Windows 7, однако в последней она применяется для большего количества компонент.

ELAM – функция раннего запуска защиты от руткитов, эксплоитов и вредоносных программ. За счёт этого антивирусы в Windows 8 могут запускаться в процессе загрузки ОС прежде, что позволяет им проверять драйверы, библиотеки и другие компоненты еще до их загрузки. Встроенный

«Защитник Windows» по умолчанию использует эту функцию. Управление автозагрузкой – такая возможность существовала и в «семёрке», однако для её реализации требовались знания, которые отличаются от «базовых». Вход в систему с помощью альтернативных паролей – функция, обращенная из мобильных ОС.

Создавая Windows 8 с прицелом на мобильные устройства с помощью сенсорного ввода, Microsoft вовсе заново взглянула метод выполнения входа на компьютер, также добавила возможность аутентификации с использованием графического пароля или числового PIN-кода. Естественно, для десктопа это может быть не столь актуально, но право на жизнь предоставленная функциональность имеет.

Таким образом, встроенная защита в Windows 8 является более защищенной, чем в Windows 7. Очевидно, что встроенные средства защиты Windows 8 обеспечивают высокий уровень безопасности, который достаточен для повседневной работы.

Важно ещё не забывать, что программно-аппаратные средства защиты ОС в обязательном порядке должны дополняться административными мерами защиты. К основным административным мерам относятся [5]:

1. Постоянный контроль правильности функционирования ОС. Подобный контроль комфортно реализовать, в случаях, когда ОС поддерживает автоматическую регистрацию весомых мероприятий в особом журнале.

2. Организация и поддержание адекватной политики безопасности.

3. Указывание пользователей операционной системы о необходимости соблюдения мер защищенности при работе с ОС и контроль за соблюдением данных мер.

4. Постоянное создание и обновление запасных копий программ и данных ОС.

5. Неизменный контроль перемен в конфигурационных данных и политике защищенности ОС.

Без постоянной квалифицированной помощи со стороны администратора, достоверная программно-аппаратная защита может подавать сбои. Важно, не забывать, что в конкретных ОС могут понадобиться и другие административные меры защиты информации [6].

Таким образом, главным элементом системы безопасности в операционных системах является система контроля защиты, которая допускает в режиме конкретного времени прослеживать опасность и отвечать на возникновение в сети новых устройств, автоматизировать установку и контроль современных средств защиты. Наилучший способ защиты от любых кибератак – частая актуализация программного обеспечения методом систематических обновлений. Это содействует значительному увеличению значения защищенности в операционных системах.

Список литературы

1. Ефремов, И. Информационные технологии в сфере безопасности: практикум / И. Ефремов, В. Солопова. – Оренбург: ОГУ, 2013. – 116 с.

2. Иртегов, Д.В. Введение в операционные системы: 3-е издание / Д.В. Иртегов. – Санкт-Петербург: БХВ, 2013. – 245 с.