УДК 004.451.9 **Технические науки**

Бондаренко Е.С., *студентка 5 курса электротехнического факультета, Пермский национальный исследовательский политехнический университет*

ИССЛЕДОВАНИЕ КАЧЕСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ОС WINDOWS И ОС LINUX МЕТОДОМ СРАВНИТЕЛЬНОГО АНАЛИЗА

Аннотация. В статье рассматриваются особенности двух наиболее популярных операционных систем в России ОС Linux и ОС Windows. Определяется наиболее защищенная ОС методом сравнительного анализа по выбранным критериям.

Ключевые слова: операционная система (ОС), вредоносная программа, Linux, Windows, пользователь, обеспечение безопасности, утилита.

Abstract. In this article the characteristic of the two most popular operation system in Russia OS Linux and OS Windows is considered. The most protected operation system is determined by the method of comparative analysis by selected criterions.

Keywords: operation system (OS), malware, Linux, Windows, user, security procuring, utility.

С развитием информационных технологий все большую цену приобретает информация. Как большие корпорации дорожат своими уникальными бизнес-решениями, так и обычный пользователь ПК желает сохранить в тайне свои личные данные. К сожалению, часто неопытный пользователь может стать жертвой вредоносной программы, просочившейся посредством сети Интернет на ПК. Личные данные пользователя могут быть скомпрометированы или же вовсе зашифрованы таким образом, что пользователь потеряет к ним доступ.

Однако таким же способом вредоносная программа может проникнуть в недостаточно защищенную операционную систему ПК сотрудника какого-либо предприятия, что приведет в итоге не просто к неприятностям, но и большому

финансовому убытку. Поэтому первое, что стоит на страже Вашей информации – это операционная система.

Операционную систему (ОС) можно связывающим звеном между пользователем и аппаратным обеспечением. ОС скрывает от пользователя сложные ненужные подробности взаимодействия с аппаратурой, образуя прослойку между ними [1].

Две самые распространенные в России и конкурирующих между собой ОС – это ОС Linux и ОС Windows. Они обе используются рядовыми пользователями, в частном бизнесе и даже в государственных учреждениях, поэтому объектом исследования в данной статье стали именно эти ОС.

Изучая новости на информационных порталах антивирусного продукта Dr.WEB [2] и Лаборатории Касперского [3], можно заметить, что с конца 2015 года новые вредоносные программы появляются как для ОС Linux, так и для ОС Windows. Однако, мнения среди экспертов расходятся. Некоторые считают, что на ОС Windows совершается больше информационных атак вследствие того, что приходится инсталлировать большое число программ. Другие утверждают, что ОС Linux более уязвима к вредоносным атакам вследствие своего открытого кода.

Для более глубокого понимания проблемы обеспечения безопасности обеих изучаемых ОС, необходимо разобраться в особенностях устройства и функционирования каждой.

Особенности ОС Windows:

- *В прошлом ОС Windows – это однопользоваьельская система.* ОС Windows совсем недавно стала многопользовательской. Раньше ОС не изолировала пользователей и приложения от критически значимых объектов, что запросто могло привести к компрометации информации с помощью вредоносных программ.
- *ОС Windows монолитна по своей архитектуре.* В Windows многие программы, например, такие как Internet Explorer, Outlook, интегрированы в саму операционную систему. В следствии этого возникает неприятный каскадный эффект: если существует брешь в Internet Explorer, то она так же возникает во множестве других приложений, которые неявно для пользователя используют Internet Explorer.

- *В ОС Windows слишком широко используется RPC-механизм.* Аббревиатура RPC означает "удаленный вызов процедуры" (Remote Procedure Call). RPC-механизмы — это потенциальная угроза безопасности, поскольку их предназначение — позволить компьютерам, находящимся где-то в сети, давать данному компьютеру указания выполнить те или иные действия.

Особенности ОС Linux:

- *ОС Linux изначально была разработана как многопользовательская система.* В ОС Linux заложен принцип изолирования пользователей от приложений, файлов и каталогов, воздействующих на операционную систему в целом.
- *По своей архитектуре ОС Linux является модульной системой.* Модульная система – это такая система, в которой функции распределены по нескольким уровням, причем каждый уровень имеет ограниченный доступ к другим уровням. Следовательно, в Linux брешь в процессе какого-либо приложения уже не представляет опасности для других приложений в системе, так как практически никакие другие приложения не зависят от данного, кроме него самого.
- ОС *Linux не зависит от RPC-механизма.* В большинстве дистрибутивов ОС Linux программы инсталлируются так, что по умолчанию доступ в сеть отключен. Даже если некоторые Linux-приложения по умолчанию используют сеть, они чаще всего сконфигурированы так, что могут отвечать только локальному компьютеру и игнорируют любые запросы других компьютеров в сети [4].

Для реализации сравнительного анализа необходимо выбрать наиболее значимые критерии, обеспечивающие безопасность в обеих изучаемых ОС. В данной статье выбраны следующие критерии:

- Контроль учетных записей пользователя;
- Поддержка со стороны разработчиков;
- Шифрование жестких дисков;
- Контроль используемого ПО;
- Аудит событий;
- Блокирование сетевых угроз;
- Браузер.

В Таблице 1 представлены критерии, по которым происходит сравнение ОС, утилиты и механизмы, обеспечивающие выполнение данных критериев в каждой из ОС, а так же лидирующая по данному критерию ОС.

Таблица 1 – Сравнение обеспечения безопасности ОС Windows и ОС Linux

Критерий	ОС Windows	ОС Linux	Преимущество
Контроль учетных записей пользователя	User Account Control выдает сообщение на подтверждение действий	Разграничение пользователей на группы с различными полномочиями	ОС Linux
Поддержка со стороны разработчиков	Центр поддержки Windows: информирует о проблемах в безопасности и других значимых событиях	Центр справки и поддержки; доступен только при наличии приобретенной версии	ОС Windows
Шифрование жестких дисков	• BitLocker: встроенная программа; • TrueCrypt дополнительня утилита	• Loop-AES • TrueCrypt	Одинаково
Контроль используемого ПО	Технология AppLocker: возможность вести аудит запускаемых программ, разграничивать доступ	При установке приложения указываются группы, уполномоченные работать с данным приложением	Одинаково
Аудит событий	Необходима настройка политики аудита	System Log (системный журнал), вызываемый с помощью комбинации клавиш Ctrl+F12. Регистрируются любые события	ОС Linux
Блокирование сетевых угроз	Наличие Брандмауэра, фильтрующего и входящий, и исходящий трафик. Легко отключается в настройках	Iptables – брандмауэр, являющийся частью ядра системы. Сложен для конфигурации	ОС Linux
Браузер	Internet Explorer 8 - характеризуется развитыми средствами обеспечения безопасности	В большинстве версий – Mozilla Firefox, содержит встроенную функцию усиленной безопасности	ОС Linux

Как видно из Таблицы 1, ОС Linux содержит лучшие механизмы по обеспечению безопасности. Многие из них являются стандартными приложениями и функциями в ОС, что говорит о том, что разработчики ОС Linux лучше понимают природу вредоносных программ.

Подводя итог, важно заметить, что выбор ОС во многом зависит от личных предпочтений. Хотя ОС Linux и является более защищенной ОС, переход на данную ОС может оказаться довольно трудным из-за непривычного интерфейса. Многие проблемы в безопасности ОС Windows решаются с помощью дополнительных утилит, таких как антивирусные программы, программы против шпионства,

межсетевые экраны и т.д. Однако для предприятия это может оказаться не дешево, а среднестатистическому пользователю может не хватить опыта в установке и настройке программ. Поэтому выбор ОС остается лично за пользователем.

Библиографический список

1. Информационный портал StudFiles – [Электронный ресурс]. – URL: http://www.studfiles.ru/preview/2714844/page:3/ (дата обращения 13.08.2016).

2. Официальный сайт антивирусного продукта Dr.WEB – [Электронный ресурс]. – URL: http://news.drweb.ru/show/review/?i=9861 (дата обращения 15.08.2016).

3. Информационный портал АО «Лаборатория Касперского» – [Электронный ресурс]. – URL: https://securelist.ru/analysis/malware-quarterly/28455/it-threat-evolution-in-q1-2016/ (дата обращения 15.08.2016).

4. Информационный портал CIT Forum – [Электронный ресурс]. – URL: http://citforum.ru/security/articles/win_lin/#AEN92 (дата обращения 16.08.2016).