Содержание:

Введение

Microsoft Windows XP, в свое время, была революционной операционной системой, в том числе, с точки зрения безопасности. В каждом новом пакете обновлений (service pack) защитные функции постоянно добавлялись и улучшались. Но с прекращением выпусков пакетов обновлений безопасность этой операционной системы, фактически, остановилась на месте и новые обновления касались только исправления ошибок в операционной системе и браузере и небольших улучшений общего уровня защиты. Чего нельзя сказать об угрозах безопасности, которые эволюционируют и растут постоянно. 8 апреля этого года официально завершился срок поддержки операционной системы Windows XP и с этого момента обновления не выпускаются, что означает отсутствие даже базовой защиты, которая держалась на выпуске обновлений. Не смотря на всю серьезность ситуации, по данным исследователей из NetMarketshare, Windows XP до сих пор установлен более чем на 25% компьютеров в мире, а по результатам опросов компании «Телеком Дейли» в России это число достигает 40% среди бизнес-пользователей, при этом более половины компаний не планируют в ближайшее время переходить на более новые версии Windows. При этом практически 100% представителей бизнеса не понимают, какие проблемы могут возникнуть из-за использования неподдерживаемой устаревшей операционной системы. В нашем предыдущем обзоре был использован статистический подход к рассмотрению этого вопроса, теперь стоит взглянуть на проблему с практической стороны. Риски продолжения использования Windows XP колоссальны и чтобы это продемонстрировать, необходимо сравнить защитные механизмы Windows XP и современных операционных систем от Microsoft. В данной статье рассмотрены основные угрозы безопасности рабочих станций и проанализирована способность защитных механизмов Windows XP Service Pack 3 и Windows 8.1 противостоять этим угрозам.

Группы защитных механизмов и угрозы безопасности.

Все защитные механизмы можно условно разделить на три основных категории: обеспечение безопасности учетных записей и разграничение доступа, защита от вредоносного программного обеспечения и отражение внешних атак. Рассмотрим эти категории и перечень основных угроз, защиту от которых они обеспечивают: Безопасность учетных записей– к этой категории относятся механизмы, позволяющие обеспечить разграничение доступа, авторизацию и защиту от внутреннего нарушителя и должны обеспечивать защиту от следующих угроз: Подбор и взлом паролей; Получение пароля пользователя (подсматривание, социальная инженерия); Несанкционированный доступ к файловым объектам и реестру Windows; Прямой доступ к файловым объектам из другой операционной системы или путем снятия носителя информации и подключения к другому компьютеру; Утеря и кража носителей информации. Защита от вредоносного программного обеспечения– к этой категории относятся механизмы, обеспечивающие противодействие вредоносной активности программного обеспечения и позволяющие заблокировать доступ к критичной информации, перехвату управления и другим несанкционированным действиям. В этой же категории рассматриваются угрозы, направленные на автоматизированное распространение вредоносных программ и заражение других компьютеров. Актуальные угрозы в данной категории: Заражение загрузочного сектора; Перехват паролей при входе в Windows и подмена экрана загрузки; Запуск вредоносного кода через эксплуатацию уязвимостей типа «переполнение буфера» в компонентах операционной системы и стороннего программного обеспечения; Вредоносное программное обеспечение, запускаемое пользователем; Перехват исполнения стандартных функций операционной системы; Вредоносное программное обеспечение, функционирующее как драйвер; Подмена служебных файлов и библиотек. Отражение внешних атак– категория, к которой относится противодействие вторжений из локальной сети и сети Интернет со стороны внешних нарушителей. Данная категория должна обеспечивать нейтрализацию следующих угроз: Эксплуатация уязвимостей в сетевых сервисах операционной системы; Несанкционированный удаленный доступ; Сканирование портов и анализ установленного программного обеспечения; Атаки на пользователя через веб-браузер (подделка страниц платежных систем, подталкивание к запуску вредоносных программ и т.д.).

1.

Безопасность учетных записей и разграничение доступа.

Последняя версия Windows XP располагает следующими защитными механизмами: Авторизация и вход в систему – в этой области Windows XP предлагает свой механизм “Windows Logon”, который обеспечивает идентификацию и аутентификацию пользователей, вся парольная информация в Windows XP шифруется, реализована поддержка смарт-карт и токенов для авторизации. Реализованные механизмы позволяют обеспечить защиту от подбора паролей и, с помощью альтернативных идентификаторов, от несанкционированного получения пароля пользователя. Но в Windows XP не обеспечен должный уровень защиты хранимых паролей, используются слабые алгоритмы шифрования, из-за чего существуют способы относительно быстрого взлома паролей, при наличии доступа к объектам, в которых хранятся зашифрованные пароли.

Windows XP способна обеспечить полноценную защиту от несанкционированного доступа к файловым объектам и реестру. Основным недостатком системы разграничения доступа является установка прав администратора для пользователя по-умолчанию. Это приводит к тому, что большинство пользователей после установки операционной системы продолжают использовать административный аккаунт и разграничение доступа, фактически, не выполняет своих функций. Но при правильной настройки механизмы полностью выполняют возложенные на них функции по защите. Политики безопасности – включают в себя политики пользователей, политики безопасности и политики аудита. Наборы настроек, позволяющих гибко настроить уровень защищенности операционной системы.
Windows XP способна обеспечить полноценную защиту от несанкционированного доступа к файловым объектам и реестру. Основным недостатком системы разграничения доступа является установка прав администратора для пользователя по-умолчанию. Это приводит к тому, что большинство пользователей после установки операционной системы продолжают использовать административный аккаунт и разграничение доступа, фактически, не выполняет своих функций. Но при правильной настройки механизмы полностью выполняют возложенные на них функции по защите. Политики безопасности – включают в себя политики пользователей, политики безопасности и политики аудита. Наборы настроек, позволяющих гибко настроить уровень защищенности операционной системы.

Разграничение доступа – как и в Windows XP, поддерживается для объектов файловой системы и для системного реестра. Благодаря разделению административных и пользовательских учетных записей, работа под аккаунтом администратора практически исключена. При этом доработаны механизмы повышения привилегий по требованию.

Политики безопасности – данные механизмы были расширены, увеличилось число доступных опций и настроек.

Windows 8.1 не только обеспечивает защиту от всех основных угроз, связанных с авторизацией пользователей и несанкционированным доступом, но и позволяет сделать это с высоким комфортом и гибкостью.

Таблица 1. Сравнение безопасности учетных записей и разграничения доступа в Windows XP SP3 и Windows 8.1

Угрозы	**Windows XP SP3**	**Windows 8.1**
Подбор и взлом паролей	Windows Logon, слабая защита	Обновленный Windows Logon, сильная защита
Получение пароля пользователя	Смарт-карты и токены	Смарт-карты, токены, вход по пин-коду, авторизация по жестам
Несанкционированный доступ к файловым объектом и реестру Windows	Разграничение доступа, только для NTFS	Разграничение доступаDynamic Access Control
Прямой доступ к файловым объектам	Encrypting File System, только для жестких дисков	BitLocker

Утеря и кража носителей информации	Нет защиты	BitLocker To Go

3. Защита от вредоносного программного обеспечения.

Windows XP в своей истории пережила не одну эпидемию компьютерных вирусов и до сих пор активно подвергается атакам со стороны «троянов», «червей» и другого вредоносного программного обеспечения. Инженеры Microsoft представили в Windows XP несколько инновационных систем, которые в последствии стали стандартом для всех операционных систем, в том числе производства других компаний. Однако, большинство из реализаций данных систем в Windows XP успешно обходится вредоносными программами, а развитие систем защиты в устаревшей операционной системе не целесообразно, поэтому на данный момент технологии защиты от вредоносного кода в Windows XP не выполняют своих прямых функций. Тем не менее, рассмотрим их подробнее: Windows Logon – обновленная (по сравнению с предыдущими версиями Windows) технология входа в систему, требующая нажатия комбинации клавиш Ctrl, Alt и Delete (комбинация, которая не может быть подделана программно). Данная технология позволяет обеспечить защиту от перехвата паролей при входе в Windows за счет невозможности внедриться в этот процесс, а также защищает от подмены экрана загрузки. Data Execution Prevention – запрет на исполнение кода из области памяти, выделенной под данные. Изначально механизм задумывался, как универсальное решение проблемы атак на переполнение буфера. Однако достаточно быстро исследователи компьютерной безопасности нашли способы обойти данную защиту в Windows XP. Software Restriction Policies – механизмы задания политики запуска программ, позволяющие минимизировать риск заражения вирусами за счет блокировки их запуска. На нашем сайте есть обзор данного механизма. По-умолчанию данный защитный механизм выключен, а его настройка требует серьезных знаний в области системного администрирования, поэтому рассматривать данный механизм можно только для решения частных задач, а не универсального решения для защиты от вредоносного программного обеспечения. Центр обеспечения безопасности (Windows Security Center) – инструмент для

управления безопасностью системы, в который интегрированы служба обновлений (Windows Update), управление встроенным брандмауэром и сторонними антивирусными продуктами. Благодаря реализации Windows Update и частому выпуску исправлений безопасности, разработчикам вредоносного программного обеспечения приходилось постоянно искать новые ошибки в операционной системе и обновлять свои вредоносные коды. Этот механизм успешно снижал количество действующих вредоносных программ и усложнял их распространение. Но с окончанием поддержки этот механизм перестал выполнять свои функции стал полностью бесполезным.

В Windows XP нет необходимых механизмов для контроля и защиты загрузочного сектора, нет эффективной защиты от уязвимостей типа «переполнение буфера», также как нет защиты от запускаемого пользователем вредоносного программного обеспечения и других угроз со стороны вредоносного программного обеспечения. Таким образом, Windows XP, даже со всеми последними обновлениями, практически беззащитна перед вредоносными программами. И, стоит отметить, что даже с наложенными антивирусными решениями, данная проблема не решается полностью. Без поддержки со стороны операционной системы, антивирусные программы не в состоянии справиться с полным перечнем угроз. В Windows 8.1 перечень защитных механизмов и использованных технологий гораздо больше, многие из которых пришли из предыдущих версий Windows – Vista и 7, и были улучшены и доработаны до современных реалий. В нашей недавней публикации были подробно описаны данные защитные механизмы, но давайте взглянем на них еще раз: Доверенная загрузка – с помощью поддержки Unified Extensible Firmware Interface (UEFI) и реализации технологии Secure Boot обеспечивается возможность запуска только оригинального ядра операционной системы и подписанных производителями драйверов. Таким образом, выполнение недоверенного программного кода в процессе загрузки полностью исключается, также исключается заражение загрузочного сектора и внедрение вредоносного кода в драйверы. Кроме того, с помощью технологии Secure Boot возможно восстановление файлов операционной системы, поврежденных вредоносным программным обеспечением. Контроль учётных записей пользователей (User Account Control) – механизм подтверждения опасных действий со стороны пользователя. Программное обеспечение не может обойти UAC в Windows 8.1 (для некоторых других версий операционных систем Windows существуют известные способы обхода) и выполнить вредоносное действие без подтверждения пользователем. При этом, даже если пользователь работает по административной учетной записью, UAC защищает операционную систему от действия программ,

запущенных пользователем. Data Execution Prevention (DEP) – впервые созданная в Windows XP технология активно развивалась и усиливалась, в Windows 8.1 данная технология позволяет защитить не только саму операционную систему, но и стороннее программное обеспечение. Риск реализации атак типа «переполнение буфера» многократно снижается, при включенной защите с помощью DEP. SEHOP – механизм предотвращения вмешательства вредоносных программ в средства структурной обработки исключений (SEH). AppLocker – логическое продолжение технологии Software Restriction Policies, в Windows 8.1 технология AppLocker позволяет настроить правила запуска приложений, ограничить выполнение неучтенных программ и даже ограничить работу нелицензионного программного обеспечения. Как и SRP, функции AppLocker по-умолчанию выключены, но их настройка не представляет большого труда, особенно, если компьютер функционирует в составе домена. Address Space Layout Randomization (ASRL) – технология случайного изменения расположения важных структур в адресном пространстве, впервые выпущенная в Windows Vista, активно поддерживается в Windows 8. В Windows XP расположение важных частей (образов исполняемых файлов, подгружаемых библиотек, кучи и стека) в оперативной памяти не менялось и вредоносным программам было несложно подменить нужные функции и данные с помощью прямого доступа к памяти. В Windows 8.1 все данные в оперативной памяти перемешены и изменяются как при перезагрузке, так и в процессе работы. Благодаря этому, вредоносный код не может найти нужные участки памяти и изменить работу системных функций и загруженного кода. Защитник Windows – это встроенное антивирусное решение, позволяющее защитить операционную систему от вредоносного и нежелательного программного обеспечения, в том числе обеспечивается защита от программ типа «rootkit». Защитник Windows в новой Windows 8/8.1 – это бывший Microsoft Security Essentials, который теперь встроен в операционную систему по умолчанию. Он обладает достаточным базовым антивирусным функционалом, позволяющим пользователям первое время не пользоваться сторонним антивирусом. Хотя для полноценной защиты рекомендуется установить профессиональный антивирусный продукт, у которого эффективность работы гораздо выше. Центр поддержки – современная замена центру обеспечения безопасности. Центр поддержки контролирует и управляет работой Защитника Windows, технологией Smart Screen (о ней – ниже), брандмауэром и обновлениями операционной системы. Защитные механизмы Internet Explorer – браузер, поставляющийся в комплекте с Windows 8, оснащен различными защитными механизмами, предотвращающими внедрение вредоносного программного обеспечения через посещаемые пользователем сайты.

В число таких механизмов входят режим защищенного исполнения расширений, HTML5-песочница (sandbox), расширенный режим защиты, ограничивающий полномочия браузера в системе и многие другие. Подробнее вопросы защиты от внешних угроз, в том числе от веб-угроз, рассмотрены в следующем разделе.

Таблица 2. Сравнение защиты от вредоносного программного обеспечения в Windows XP SP3 и Windows 8.1

Угрозы	**Windows XP SP3**	**Windows 8.1**
Заражение загрузочного сектора	Нет	Unified Extensible Firmware Interface, SecureBoot
Перехват паролей при входе в Windows и подмена экрана загрузки	Windows Logon, слабая защита	Обновленный Windows Logon, сильная защита
Эксплуатация уязвимостей типа «переполнение буфера»	Data Execution Prevention, слабая защита	Обновленная Data Execution Prevention, сильная защита
Вредоносное программное обеспечение, запускаемое пользователем	Software Restriction Policies, требует сложной настройки	AppLocker, Защитник Windows, AppContainter, Магазин Windows
Перехват исполнения стандартных функций операционной системы	Нет	Address Space Layout Randomization
Вредоносное программное обеспечение, функционирующее как драйвер	Нет	SecureBoot, Защитник Windows

Подмена служебных файлов и библиотек.	Нет	AppContainter, Address Space Layout Randomization, Защитник Windows

4. Отражение внешних атак.

Windows XP обладает только одним механизмом, связанным с защитой от внешних атак. Этот механизм - встроенный брандмауэр (Windows Firewall) – фильтр сетевого трафика, позволяющий фильтровать входящий сетевой трафик. Не смотря на малое количество функций и настроек, брандмауэр справляется с основной задачей – блокировки трафика из внешних источников и позволяет немного повысить уровень защиты от внешних атак. При этом он никак не защищает от удаленной эксплуатации уязвимостей и атак на пользователя через веб-браузер. Встроенная в Windows XP версия браузере Internet Explorer не предлагает никаких серьезных функций по защите и в ней постоянно обнаруживают новые уязвимости, которые, при отсутствии обновлений, не будут исправляться.
Встроенный брандмауэр в Windows 8 по функциональным возможностям значительно обходит брандмауэр в Windows XP. Кроме стандартной фильтрации входящего трафика, появились функции управления исходящим трафиком, активный мониторинг текущего трафика, а также встроенное управление правилами безопасности подключений IPSec и многие другие функции. Благодаря значительному расширению функциональности, брандмауэр Windows 8 может справиться с большинством сетевых угроз самостоятельно, в том числе с угрозами перехвата и подделки трафика.

Smart Screen – комплексное решение по защите пользователя во время посещения вебсайтов и других Интернет-сервисов. В состав Smart Screen входят три механизма – антифишинговая защита, проверка репутации загружаемых приложений и защита от загружаемых вредоносных программ. Под Windows 8/8.1 Smart Screen работает как в самом браузера, так и независимо от него, на уровне операционной системы.

С помощью механизма антифишинговой защиты, все сайты, которые пытается посетить пользователь, проверяются по специальной централизованной базе. Если на сайте были обнаружены поддельные формы авторизации, повторяющие формы различных сервисов (банки, магазины, платежные системы и т.д.), он заносится в

общую базу. При попытке пользователя открыть такой сайт, доступ к нему блокируется с выводом предупреждения. Также под действие фильтра попадают сайты с известными вредоносными кодами и программным обеспечением. Репутационная проверка загружаемых файлов позволяет опознать файл после его загрузки и оценивает его опасность или безопасность для пользователя, основываясь на подписи файла, количестве его загрузок другими пользователями и попытками осуществить подозрительные и вредоносные действия на других компьютерах. Если файл признан не надежным, его запуск блокируется, пользователю выводятся специальные предупреждения о возможном вредоносном действии скачанного файла. Защита от вредоносных программ действует по принципу антифишинговой защиты – загруженные файлы проверяются по контрольным суммам в глобальной базе данных и, если файл в базе значится как вредоносный, пользователю выводится предупреждение, а запуск файла блокируется. Обновления браузера распространяются вместе с обновлениями операционной системы, поэтому пользователь при работе с вебсайтами максимально защищен и не рискует, заходя на незнакомую страницу, содержащую вредоносный код, даже если она еще не числиться в базе фишинга. Браузер Internet Explorer, входящий в состав Windows 8.1, максимально защищает пользователя не только от опасных сайтов и программ, но и обладает сильными функциями самозащиты, в которые входит контроль плагинов, расширений и ActiveX-компонентов. Таким образом, блокируются попытки вредоносных программ встроиться в браузер и получить доступ к Интернет-активности пользователей. Windows 8.1 имеет все необходимые инструменты для полноценной защиты пользователя от внешних атак и угроз, исходящих из сети Интернет. Усилив встроенные защитные механизмы внешним сетевым фильтром или комплексным антивирусным решением, можно добиться полной защиты от всех возможных угроз.

Таблица 3. Сравнение отражения внешний атак в Windows XP SP3 и Windows 8.1

Угрозы	**Windows XP SP3**	**Windows 8.1**
Эксплуатация уязвимостей в сетевых сервисах операционной системы	Нет	Обновления операционной системы

Несанкционированный удаленный доступ	Брандмауэр Windows	Брандмауэр Windows
Сканирование портов и анализ установленного программного обеспечения	Брандмауэр Windows	Брандмауэр Windows
Атаки на пользователя через веб-браузер	Нет	Smart Screen, встроенные механизмы Internet Explorer, обновления браузера в составе обновлений операционной системы

5. Улучшения безопасность Windows 8.1.

Прогрессивные технологии постоянно развиваются, к чести разработчиков, в лучшую сторону. Если вы поклонник операционных систем от Microsoft, то наверняка еще с выхода Windows 95 вас всегда, с каждой новой версией и каждым обновлением беспокоил вопрос безопасной работы и антивирусного ПО. Нужно сказать откровенно, что в компании очень серьезно, мягко говоря не дорабатывали эту часть функционала и в каждой ОС было очень много багов.

Так повторялось до появления операционных систем восьмой линейки. Особенно улучшена **безопасность Windows 8.1**, параметры которой заставляют кардинально пересмотреть мнение пользователей об этой операционной системе и серьезно задуматься приверженцев XP или семерки о переходе на эту ОС.

В подтверждение того, что вся новая восьмая линейка операционных систем действительно самая лучшая из предыдущих версий с точки зрения безопасности за все время существования Microsoft, можно привести опубликованный недавно отчет лаборатории Microsoft Security Intelligence Report. Здесь приводятся данные, подтверждающие, что в сравнении с ОС Windows 7 в новых системах уровень безопасности увеличен в 6 раз. Сравнительная информация, касающаяся XP, впечатляет больше – она была слабее в параметрах защиты в 20 раз! Стоит задуматься.

Безопасность Windows 8.1.

Безопасность Windows 8.1 построена на политике и логическом продолжении программного кода версии 8.0, с добавлением к ним еще несколько полезных функций. Анализируя изменения в коде можно сделать вполне обоснованный вывод, что потенциал защиты до конца не исчерпан, и в будущем можно ожидать действительно революционного прорыва – стопроцентной гарантии защиты компьютера от внешних угроз. И это не иллюзорная мечта, достижения которой так долго ждут все владельцы ПК и ноутбуков. Ниже мы попробуем подтвердить выводы программистов, рассмотрев три наиболее важных направления в защите:

•Шифрование устройств,

•Возможность поддержки новых технологий биометрических интерфейсов,

•Функционал выборочного полного уничтожения данных.

Шифрование информации в системе безопасности Windows 8.1.

В обеспечении полноценного шифрования в новых ОС задействован потенциал BitLocker (в версии RT без управления и автоматическим шифрованием всего диска). Появление 8.1 весь функционал BitLocker вывело на совершенно иной уровень качества. Это видно уже из того, что его намного легче и проще настроить рядовому пользователю непосредственно под более конкретизированные личные задачи. Причем развертывание самого BitLocker выполняется в 20 раз быстрее, чем в предыдущих вариантах. Особенно это заметно тем, кто уже сейчас пользуется жесткими дисками последних поколений – процедура полного шифрования выполняется менее, чем за 1 секунду!

Для улучшения **безопасности Windows 8.1** функция полнодискового шифрования работает автоматически (это распространяется и на обычные 8.0 и RT, обновленные до 8.1). Защита методом шифрования устанавливается уже при установке ОС на компьютер сразу после первого входа под учетной записью с правами администратора. Смысл самой идеи действительно привлекательный. В Microsoft планируют, что шифрование по умолчанию всех устройств в будущем

станет обязательной частью политики безопасности и у пользователей вообще отпадет необходимость заморачиваться с этим процессом самостоятельно, настраивая какие-либо функции через панель управления.

Уничтожение данных в Windows 8.1.

Особенно актуальны новые возможности по полному уничтожению данных в Windows 8.1 для бизнес-среды. С учетом того, что в последние годы во всем мире развивается тенденция удаленной работы с корпоративной информацией или использование на рабочем месте личных электронных устройств (BYOD), это делает жизнь спокойнее и владельцам компаний и пользователям. Предусмотренное в 8.1 выборочное удаление (Selective Wipe) достаточно настроить на уничтожение только информации общего пользования, не затрагивая при этом личные данные и файлы.

Технологически такое решение обеспечивается установленным еще на 8.0 функционалом Exchange ActiveSync (EAS). Работает с возможностью режима удаленного стирания. При этом уже на 8.1 задана возможность поддержки нового стандарта OMA-DM (Open Mobile Alliance Device Management).

Пока система **безопасности Windows 8.1** способна поддерживать только уничтожение корпоративных данных для почтовых клиентов и в Рабочих папках. Есть еще одна функция, но она работает только с использованием версии Server 2012 непосредственно на стороне самого сервере. Разработчики планируют существенно увеличить функционал выборочного затирания уже в ближайших выпусках обновлений.

Технологии управления удаленным доступом и безопасность.

Компания Microsoft с выводом на рынок Windows 8.1 начала практически осуществлять политику отказа от использования паролей в обеспечении удаленного доступа. Привычный всем способ поэтапно уходит в прошлое и уступает место более современным технологиям для управления удаленным доступом. Старт этому процессу был дан еще в первой восьмерке функцией поддержки многофакторной аутентификации пользователя с правом доступа через

смарт-карты.

В рассматриваемой нами операционной системе 8.1 сделан следующий шаг – ОС поддерживает новое поколение биометрических интерфейсов (сканеры отпечатков пальцев). Это принципиально изменяет все привычные нам способы аутентификации в пользу новых технологий, существенно увеличивая уровень **безопасности Windows 8.1** при удаленном управлении с использованием Сети, которая кишит программами шпионами и другими злонамеренными кодами на сайтах и блогах.

Конечно, Windows 8.1 не ограничена только рассмотренными нами функциями, которые вывели ее безопасность на новый уровень надежности. Если вам интересна эта тема – оставляйте свои комментарии, делитесь своим опытом. Ваше мнение, особенно личные примеры, всегда ценны для нас. Мы же в следующих статьях обязательно ответим на наиболее актуальные ваши вопросы.
Эту статью так же ищут по запросам: оптимизация windows 8.1, настройка windows 8.1.

Выводы

Microsoft Windows XP обладает многими защитными механизмами и в момент своего появления и развития по праву считалась операционной системой с высокой степенью защищенности. Но технологии не стоят на месте, злоумышленники и разработчики вредоносного программного обеспечения постоянно ищут новые способы обхода защитных функций операционных систем. Во время активного развития, Windows XP могла противостоять постоянному натиску. Это особенно видно, если сравнить количество защитных функций в первой версии Windows XP и в версии с третьим пакетом обновлений. Но с началом разработки следующей версии Windows, развитие XP в целом остановилось, регулярно выпускаемые обновления лишь закрывали обнаруженные уязвимости, но не позволяли адекватно повышать уровень защиты. С окончанием периода поддержки Windows XP обновления перестали выпускаться и текущий уровень защищенности данной операционной системы не может считаться даже базовым. Фактически, можно считать, что Windows XP беззащитен. Даже установка комплексных антивирусных средств и других средств защиты информации, не может полностью решить проблему защиты, так как в задачи данных средств не входит обнаружение и закрытие уязвимостей операционных систем. Напротив, Windows 8.1 является

максимально защищенной из всех операционных систем от Microsoft. В Windows 8.1 входят механизмы защиты, которые разрабатывались и оттачивались годами в версиях Windows XP, Vista и 7, а также новые инновационные защитные комплексы. Благодаря полному охвату всех видов защиты, Windows 8.1 обеспечивает высокий уровень нейтрализации угроз даже без дополнительных средств. А с помощью антивирусов и других средств защиты информации, Windows 8.1 становится максимально защищенной средой. Учитывая все возрастающие оценки экспертов по финансовым и репутационным потерям компаний в следствие компьютерных атак и заражений вредоносными программами, обновление на Windows 8.1 обойдется гораздо дешевле, чем ущерб от использования Windows XP. В данной статье не рассмотрены другие аспекты использования устаревшей среды, например, не совместимость с современным программным обеспечением и низкие функциональные и пользовательские возможности Windows XP. Организациям и пользователям, продолжающим использовать Windows XP следует объединить все факторы в пользу Windows 8.1 и принять решение о переходе как можно скорее.