УДК 004.056

НАСТРОЙКИ КОНФИГУРАЦИЙ БЕЗОПАСНОСТИ В WINDOWS

О. А. Николаенкова, А. А. Серик, Р. Э. Хагуш
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Аннотация. Современные технологии не стоят на месте. Вот и на смену всем уже ставшей привычной Windows 10 пришла свежая Windows 11. Она отличается от своей предшественницы не только изменениями в интерфейсе, который стал более приятным и свежим, но и множеством дополнительных функций. Эти функции не так заметны для обычного пользователя, поэтому требуется детальное их рассмотрение для последующего активного использования. Цель авторов данного исследования — описать возможности конфигураций по обеспечению безопасности, доступные теперь в Windows 11.

Ключевые слова: операционная система, Windows, антивирусы, BitLocker, шифрование, защита, угрозы.

WINDOWS SECURITY SETTINGS

Olga A. Nikolaenkova, Artem A. Serik, Renat E. Khagush
Don State Technical University (Rostov-on-Don, Russian Federation)

Abstract. Modern technologies do not stand still. So the new Windows 11 has replaced the already familiar Windows 10. It differs from its predecessor not only by changes in the interface, which has become more pleasant and fresh, but also by a lot of additional functions. These functions are not so noticeable to the average user, so a detailed consideration of them is required for subsequent active use. The objective of the authors of this study is to describe the security configuration capabilities now available in Windows 11.

Keywords: operating system, Windows, antiviruses, BitLocker, encryption, protection, threats.

Введение. Операционная система Windows 11 отличается от предыдущих систем набором некоторых присущих ей дополнительных функций. Определить и разобраться в них предлагают авторы данной работы. В статье рассмотрена настройка конфигураций по обеспечению безопасности, показано, как настроить или отключить автоматические обновления в операционной системе, как выключить встроенный в Windows 11 антивирус, добавить в список его исключений нужные объекты. Кроме того, описана надежность и безопасность BitLocker, а также проанализированы методы его дополнительной защиты. Рассмотрены функции облачной загрузки и переустановки Windows.

Для достижения поставленной цели необходимо решить следующие задачи: определить пути настройки автообновления, рассмотреть технологию шифрования BitLocker, работу со встроенным антивирусом, шаги по добавлению программ в список исключений, настройку контроля доступа к пакетам, средства облачной загрузки и переустановки самой системы.

Основная часть. Начнем анализ Windows 11 с настройки обновления и его отключения. Обновления сами по себе выполняются в фоновом режиме и доставляются при перезагрузке устройства. Раньше обновления всегда устанавливались в самый неудобный момент, зачастую прерывая процесс взаимодействия пользователя с компьютером. Как и раньше, обновления можно посмотреть на экране «Параметры» → «Центр обновления Windows». Там же доступен журнал обновлений для получения информации об установленных ранее обновлениях и различных видах работы с ними [1, 2].

Рассмотрим процесс отключения обновления на совсем. Можно пометить соединение как лимитное, что позволит не мешать вам сообщениями про обновления при работе в системе. Здесь важно помнить, что при подключении к сети через другое соединение, не помеченное как лимитное, обновление начнет ставиться на систему. Отключать обновления или нет — дело каждого пользователя и зависит от преследуемых им целей. Приведем порядок действий: 1) командой «Win + R» вызовем диалоговое окно и запустим редактор групповой политики gpedict.msc; 2) посетим раздел «Конфигурация компьютера»; 3) далее «Компоненты Windows», затем «Центр обновления Windows», «Управление интерфейсом пользователя». В нем необходимо найти политику «Настройки автоматического обновления». Двойным щелчком левой клавиши мыши (ЛКМ) отключим политику, переведя ее в состояние «Отключено» и нажмем кнопку «ОК». После всех этих действий устройство следует перезагрузить. Данный способ отключит автоматический способ обновления, причем ручной по-прежнему будет доступен. При этом варианте пользователь сможет устанавливать обновления, когда ему это будет нужно [3].

Безопасность BitLocker. Любая операционная система имеет три аспекта: скорость работы, ее удобство и надежность. В системе Windows на пересечении этих составляющих находится BitLocker. Как правило, один из трех факторов всегда уступает, а Windows попыталось найти компромисс. С точки зрения надежности, все не так плохо, но и не идеально. Шифрование реализовано хорошо, но проблемным местом является ключ восстановления. Для расшифрования диска используется ключ, который, как правило, хранится локально. Обычным поиском ключа в файле и копированием его себе можно, применив его, расшифровать диск. Поэтому хранить ключ следует на отдельном носителе. Во избежание таких случаев следует:

1. Открыть сохраненный файл в любом текстовом редакторе, после чего почистить в нем все, кроме самого ключа. Так уже будет сложнее понять, что это за ключи и ключи ли это вообще. Для большей маскировки можно несколько раз скопировать его и заменить некоторые символы, а напротив каждой копии написать название какой-то программы, чтобы точно можно было подумать, что это серийный номер к разным программам.

2. У правильного ключа заменить одну-две цифры. И даже если вендор скопирует этот ключ и вставит в окно восстановления, открыть диск у него не получится. Главное потом — не забыть, какие цифры и на какие поменяли.

3. Не хранить ключи восстановления в учетной записи Microsoft. А есть уверенность, что Microsoft не передаст эти ключи восстановления по официальному запросу? Если все-таки ключ сохранен в ней, перейдите по адресу: https://account.microsoft.com/devices/recoverykey и удалите все имеющиеся там ключи. Впрочем, это спасет только от хакеров. А вот от самой компании Microsoft вряд ли, поскольку ваши ключи уже наверняка скопированы. Рекомендуется сменить пароли ко всем зашифрованным дискам и больше не сохранять ключи в учетной записи [4].

Таким образом, перекрыта одна из самых больших уязвимостей BitLocker. Рассмотрим следующий момент. Если отключить шифрование, все сектора останутся зашифрованными, однако пользователю этого не будет видно. На программном уровне этот процесс будет выглядеть так: загрузчик Windows получает VMK (Volume Master Key — мастер-ключ тома) из метаданных и расшифровывает все файлы, что явно ухудшает производительность [4].

Следующая уязвимость заключается в том, что ключи шифрования записываются в оперативную память, из чего следует, что из дампа памяти их можно вытащить и получить доступ. Также VMK может храниться в файле гибернации hiberfil.sys. Это означает, что, если кто-то извлечет жесткий диск из компьютера, то можно найти мастер-ключ для разблокировки BitLocker-диска. Чтобы избежать такой ситуации, следует отключить режим гибернации (команда

powercfg-h off от имени админа) и удалить файл hiberfil.sys.

Антивирусы. Конечно же, любая современная операционная система имеет свой встроенный антивирус. И защитник Windows справляется со своими задачами. Но уже сложился стереотип, что встроенные антивирусы бесполезны, поэтому все пользователи, как правило, ставят бесплатные сторонние антивирусы, которые далеко не лучше, а то и хуже встроенных. Часто возникают случаи, когда антивирус неверно определяет угрозу, что весьма мешает при взаимодействии с системой. Решением является добавление нужных программ и файлов из списка исключений, но это требует осторожности и ответственности со стороны пользователя. Для создания такого списка необходимо [3]:

1) в окне «Безопасность Windows» открыть раздел «Защита от вирусов и угроз»;

2) пролистать ниже и найти ссылку «Управление настройками», перейти по ней;

3) в самом низу экрана перейти по ссылке «Добавление или удаление исключений»;

4) кликнуть на кнопку «Добавить исключение», выбрать необходимый вам тип.

Теперь рассмотрим временное отключение антивируса, что тоже может пригодиться. Windows 11 сделали так, что антивирус невозможно отключить навсегда, оставив возможность временной деактивации. Открываем окно «Безопасность Windows». Далее ищем пункт «Защита от вирусов и угроз». В нем нажимаем «Управление настройками». И отключаем пункты «Защита в режиме реального времени», «Облачная защита», «Автоматическая отправка образцов». Далее в «Управлении приложениями/браузером» открываем «Параметры защиты на основе репутации» и деактивируем проверку и блокировку потенциально нежелательных приложений, а в свойствах самого файла, если он был скачан из Интернета, ставим отметку «Разблокировать». После чего применяем настройки.

Контроль доступа к пакетам. В Windows 11 стала доступна такая функция, как контроль доступа к папкам. Владелец имеет возможность создать список контролируемых папок. Файл, в котором хранится данный список, находится под защитой. Как только возникнет попытка его изменить, антивирус отклонит данный процесс. Даже в случаях, когда в устройство занесен вирус-шифровальщик, эта настройка позволит сохранить информацию. Рассмотрим процесс настройки [1]:

1) заходим в «Безопасность Windows» и нажимаем на «Защитник от вирусов и угроз»;

2) двигаемся в самый низ экрана и там переходим по ссылке «Управление защитой от программ-шантажистов»;

3) включаем параметр «Контролируемый доступ к папкам. Защита включена». После этого в случае попытки вируса-шифровальщика зашифровать твои данные или при других неодобренных системой изменениях в файлах пользователь будет получать уведомление о том, что недопустимые изменения заблокированы;

4) по умолчанию защищаются системные папки документов пользователей, но при желании можно перейти в раздел «Защищенные папки» → «Добавить защищенную папку» и указать любую другую папку или даже целый диск, который необходимо защитить от несанкционированных изменений. Системный диск не нужно добавлять в этот список — по понятным причинам;

5) далее просто отмечаем команду «Разрешить работу приложения через контролируемый доступ к папкам»;

6) через кнопку «Добавление разрешенного приложения» добавляем нужные нам приложения или программы.

Загрузка из облака. В одном из обновлений была добавлена функция «Загрузка из облака». Суть ее заключается в следующем: вместо привычной переустановки системы система

самостоятельно скачивает и устанавливает актуальную и необходимую версию на ваше устройство. Например, раньше для осуществления этой операции необходимо было наличие отдельного установочного носителя или обновления системы с последующим сбросом до заводских настроек, что требовало значительного количества времени. После отката система нуждалась в установке актуальных обновлений, теперь этого не требуется.

Заключение. Таким образом, рассмотрены основные возможности по работе с конфигурацией безопасности в Windows 11. Будет ли осуществлен массовый переход на 11-ю версию системы, как когда-то на 10-ю, говорить пока рано. Но ясно лишь одно: рано или поздно такой переход все же состоится, он неизбежен. Прогресс не стоит на месте. Поэтому надо уже сейчас, заранее, знакомиться с основными возможностями новой версии операционной системы Windows, изучать ее преимущества, чтобы шагать в ногу со временем, быть готовым к любым изменениям.

Библиографический список

1. Колисниченко, Д. Н. Самоучитель Microsoft Windows 11 / Д. Н. Колисниченко. — Санкт-Петербург : БХВ-Петербург, 2022. — 368 с.

2. Киприан, А. Р. Windows 11 All-in-One For Dummies. / А. Р. Киприан. — New York : Wiley, 2022 — 899 с.

3. Колисниченко, Д. Н. Microsoft Windows 11. Первое знакомство / Д. Н. Колисниченко. — Санкт-Петербург: БХВ-Петербург, 2022. — 128 с.

4. Фредрис, П. Windows 11 Simplified / П. Фредрис. — New York : Wiley, 2022 — 610 с.

Об авторах:

Николаенкова Ольга Александровна, студентка кафедры «Вычислительные системы и информационная безопасность» факультета «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), nikolaenkovaolga@bk.ru

Серик Артем Андреевич, студент кафедры «Вычислительные системы и информационная безопасность» факультета «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), artem.serik.04@mail.ru

Хагуш Ренат Эдуардович, студент кафедры «Вычислительные системы и информационная безопасность» факультета «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), reno007reno@mail.ru

About the Authors:

Nikolaenkova, Olga A., student of the Computing Systems and Information Security Department, Computer Science and Computer Engineering Faculty, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), nikolaenkovaolga@bk.ru

Serik, Artem A., student of the Computing Systems and Information Security Department, Computer Science and Computer Engineering Faculty, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), artem.serik.04@mail.ru

Khagush, Renat E., student of the Computing Systems and Information Security Department, Computer Science and Computer Engineering Faculty, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), reno007reno@mail.ru